Adrian Munteanu
Valerică Greavu-Şerban
Silviu-Andrei Pârvană

INVESTIGAȚII INFORMATICE JUDICIARE
Suport de curs

Adrian Munteanu, este absolvent al Universității AL. I. Cuza din Iași, profesor doctor la Facultatea de Economie și Administrarea Afacerilor din cadrul Universității Alexandru Ioan Cuza din Iași, (www.feaa.uaic.ro). Este de asemenea *Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), Control Objectives for Information and Related Technologies Certificate (COBIT), IT Infrastructure Library Certificate (ITIL), AccessData Certified Examiner (ACE)*și *Microsoft Certified Professional (MCP)*.
A mai publicat, în editura Polirom *„Auditul sistemelor informaționale contabile. Cadru general" (2002), „Rețele locale de calculatoare. Proiectare și administrare" (Ed. I -2003, Ed. II -2004), „Rețele Windows. Servere și clienți. Exemple practice" (2006)*. A publicat ca unic autor sau coautor articole în reviste internaționale și a participat la conferințe în domeniul auditului și securității sistemelor informaționale în Cehia, Ungaria, Germania, Austria, Turcia, Maroc, Spania. Este titularul cursurilor „Auditul sistemelor informaționale pentru afaceri", „Rețele locale de calculatoare" și „Guvernare IT".
Din anul 2003 este implicat în proiecte de audit, consultanță privind securitatea informațiilor și instruire IT&C pentru firme private, furnizori de servicii de utilitate publică și bancare. În 2007 și 2010 a fost Service Trainer Provider/Instructor al cursului CISA pentru ISACA România Chapter. Este coordonator și traducător al cadrului de referință COBIT 4.1 versiunea în limba română. Din 2010 este ISACA Academic Advocate. Poate fi contactat pe mail la adresa adrian.munteanu@feaa.uaic.ro.

Valerică Greavu-Șerban, este absolvent al Universității A. I. Cuza din Iași. Este lector la Facultatea de Economie și Administrarea Afacerilor, *Most Valuable Professional, Microsoft Certified Professional (MCP), Microsoft Office Specialist (MOS) Expert Level, TS 630* și fost administrator al rețelei FEAA. Este coautor la *„Rețele locale de calculatoare. Proiectare și administrare" (Ediția I), „Rețele Windows. Servere și clienți. Exemple practice"*.
În 2005, la Yokohama a fost semifinalist și a obținut locul IV în lume la concursul Imagine Cup, secțiunea IT General. În 2006, la Delphi a obținut locul II în cadrul aceluiași concurs. Începând cu 2007 a fost arbitru Imagine Cup alături de Rand Morimoto și Chris Amaris (Convergent Computing Ltd., www.cco.com). Astfel și-a validat competențele în domeniul tehnologiilor de tip server de la Microsoft. Începând cu 2005 împreună cu Adrian, este implicat în proiecte de audit, consultanță securitate și instruire ITC pentru firme private. Poate fi contactat pe mail la adresa valy.greavu@feaa.uaic.ro.

Silviu-Andrei Pârvană, este absolvent al Universității Al.I.Cuza din Iași**.** A studiat masterul de Sisteme Informaționale pentru Afaceri tema sa de disertație fiind orientată către domeniul Computer Forensic. A lucrat în Departamentul Server Rețea din cadrul Facultății de Economie și Administrarea Afacerilor iar în prezent la o companie de software. Poate fi contactat pe mail la adresa: silviu.parvana@feaa.uaic.ro.

© 2012 by Adrian Munteanu

Editura …..

Descrierea CIP a Bibliotecii Naționale a României:

…... – Iaşi: ……2012
Xxx p., 24 cm
ISBN: 937-xxx-xxx-x

I. Adrian Munteanu
xxx:xxx

Printed in ROMANIA

Adrian Munteanu
Valerică Greavu-Şerban
Sivliu-Andrei Pârvană

INVESTIGAȚII INFORMATICE JUDICIARE

2012

Cuprins

Introducere **7**

Capitolul 1 – Evoluția şi terminologia domeniului **8**

1.1. Scurtă istorie a evoluției investigațiilor informatice 8
1.2 Terminologie 9
1.3 Rolul calculatoarelor în realizarea infracțiunilor 10

Capitolul 2 - Proba digitală **11**

2.1 Proba digitală - definiție 11
2.2 Standarde internaţionale 11
2.3 Păstrarea probelor digitale 12
2.4 Lanţul de custodie 12
2.5 Probe volatile vs probe nevolatile 13
2.6 Manipularea probelor digitale 14
2.6 Ştergerea probelor digitale 15

Capitolul 3. Dispozitive electronice: tipologie, descriere şi probe potențiale **17**

3.1 Calculatoare 17
3.2 Dispozitive şi medii de stocare a datelor 17
3.2.1 Hard Disk 18
3.2.2. Banda magnetică 20
3.2.3. CD şi DVD 21
3.2.4. USB/Flash Drive, Memory Card 22
3.2.5. Dispozitive *handheld* 23

Capitolul 4. Fundamentele rețelelor de calculatoare **24**

4.1 Modelul OSI 25
4.2 Modelul TCP/IP 27
4.3 Infrastructura rețelei 29
4.3.1 Cartela de rețea 29
4.3.2 Medii de transmisie 30
4.4 Echipamente de transmisie a datelor 31
4.5 Adresa MAC 33
4.6 Adrese IP 34
4.7 Protocolul IP versiunea 4 (IPv4) 34
4.8 Protocolul IP versiunea 6 (IPv6) 36

Capitolul 5. Scena producerii infracțiunii informatice **37**

5.1. Securizarea şi evaluarea scenei 37
5.2. Documentarea scenei 38
5.3. Colectarea probelor 38
5.4. Ambalarea, transportul şi păstrarea probelor digitale 41

Capitolul 6. Achiziția datelor **42**

6.1 Formate de stocare a datelor pentru probele digitale 42
6.1.1. Formatul Raw 42
6.1.2. Formate proprietare furnizorilor de soluții informatice 42
6.2. Metode de achiziție a datelor 42
6.3. Protecția la scriere 43

Capitolul 7. Sistemul de fişiere şi regiştrii WINDOWS **44**

7.1. Sistemul de fişiere 44
7.2 Gestiunea Regiştrilor 54
7.3 Validarea şi discriminarea datelor 57
7.4 Protecția/blocarea la scriere 58
Capitolul 8. Poşta electronică (e-mail) 60
8.1 Client, server şi mesaj 60
8.2 Examinarea mesajelor 61
Capitolul 9: Dispozitive de stocare amovibile 67
9.1 Dispozitive USB şi Registry 67
9.2 Dispozitive portabile şi Registry 69
Studiu de caz 1 88
Studiu de caz 2 - Accesarea probelor pe niveluri 98
Accesul fizic la calculator 98
Accesul la secventa de boot 98
Accesul la sistemul de operare 99
Utilitare de creare a imaginilor 100
Utilitare de recuperare de date 100
Utilitare pentru eliminarea diverselor parole Windows 101
Accesul la fisiere 101
Accesul la jurnale 101
Glosar de termeni 104
Bibliografie **.....** Error! Bookmark not defined.

Introducere

După mai bine de 10 ani de când am publicat în Editura Polirom prima mea carte, am ajuns să recidivez şi să mă întorc la *prima dragoste*. Şi asta datorită, în principal, faptului că între timp meseria de *auditor de sisteme informaţionale* a început să prindă contur şi în România. Mai ales ca urmare a apariţiei unor cerinţe prin diverse acte normative (ex. OMF 1077/2003, OCMTI 389/2007, BASEL II, decizii sau instrucţiuni ale CNVM, BNR). În anii care s-au scurs de atunci, pe lângă ceva păr alb, sper că am mai acumulat şi experienţă practică alături de bunul meu coleg Valy.

CSI: Crime Scene Investigation. Un serial pe care unii dintre dumneavoastră l-aţi urmărit. Un serial în care vedem nu doar poliţişti ce urmăresc infractori ci o echipă de specialişti în diferite ştiinţe investigative. Inclusiv în investigarea infracţiunilor informatice. Am putea spune că acest material se doreşte a fi *CSI – Computer Scene Investigation.* Ar fi însă prea mult pentru demersul nostru, chiar dacă ne place cum sună. În plus, viaţa nu este ca în filme.

Pentru CINE am scris totuşi această carte? Pentru toţi cei care au nevoie de colectarea, analizarea şi păstrarea probelor digitale/electronice în meseria lor. Fie că sunt poliţişti, avocaţi, procurori sau auditori de sisteme informaţionale. Sau chiar simpli oameni pasionaţi să descopere lucruri noi.

Despre CE am scris? Aici răspunsul credem că este ceva mai dificil. În primul rând *am încercat* să scriem despre unele probleme cu care te poţi întâlni în *practică.* Şi cum practica diferă de la caz la caz, nu ne-am propus să epuizăm toată cazuistica. Am pornit de la practica *noastră, d*e la experienţele noastre din ultimii 10 ani. Nu uitaţi că locurile sunt diferite şi oamenii sunt unici. Tehnologia este într-o evoluţie continuă. Prin urmare nu trebuie să gândim în modele aplicabile în orice condiţii. Generalizările dăunează grav! Amintim că am scris din perspectiva IT-istului fără a avea pretenţia că am găsit un limbaj comun cu domeniul juridic, chiar dacă am încercat de mai multe ori să îl înţelegem.

Materialul nostru prezintă lucruri elementare din domeniul investigaţiilor informatice şi se adresează în primul rând celor care nu au o pregătire tehnică avansată ci doar cunoştinţe minimale din domeniul tehnologiilor informaţionale. Cu siguranţă acest material are defecte şi lipsuri. Măcar suntem conştienţi de acest lucru.

Am încercat să fim cât mai concişi şi să nu ne pierdem în amănunte. Sperăm ca cele ce urmează să mai împrăştie din marasmul cu care este înconjurat acest domeniu pe meleagurile noastre. Nu garantăm succesul pentru că această carte a apărut doar din credinţa că *înainte de a cere, trebuie să dai.*

Iaşi, martie 2012

Capitolul 1. Evoluția și terminologia domeniului

În ultimii 20 de ani am asistat la dezvoltarea unui nou tip de infracțiuni: cele realizate în universul digital – cyberspace. La nivel internațional remarcăm nevoia în creștere de investigare a unor infracțiuni realizate în totalitate sau parțial cu ajutorul calculatoarelor și rețelei Internet. Evoluția tehnologică tinde să ne demonstreze că și în cazul unor infracțiuni, să le spunem „clasice", investigatorul ajunge să se intersecteze cu un sistem de calcul.

1.1. Scurtă istorie a evoluției investigațiilor informatice

Pentru un domeniu aflat într-o dezvoltare exponențială, cum este cel al tehnologiilor informaționale, este dificil de identificat în mod riguros originea primelor investigații informatice. Literatura de specialitate menționează ca inițiatori ai domeniului agențiile din SUA responsabile cu aplicarea legii[1], care la sfârșitul anilor 1980 începutul anilor 1990, au dezvoltat un program comun de instruire în acest domeniu (Eoghan 2004).

Cele mai importante repere temporale sunt sintetizate mai jos:

1984 – FBI înființează "Magnetic Media Program" care ulterior devine "Computer Analysis and Response Team" (CART2)
1993 – are loc prima conferință ce tratează domeniul probelor digitale, denumite la acea vreme "computer evidence".
1995 - se înființează International Organization on Computer Evidence (IOCE3)
1998 – Interpolul organizează simpozionul "Forensic Science"
2000 – se înființează FBI Regional Computer Forensic Laboratory
2004 – Convenția Europeană cu privire la Cybercrime4

Dezvoltările uluitoare din domeniul tehnologiilor informaționale sunt cele care au condus la nevoia de specializare: profesioniști capabili să identifice, colecteze și analizeze probe digitale.

Probele electronice/digitale nu reprezintă altceva decât informații și date cu valoarea investigativă și care sunt stocate, transmise sau recepționate cu ajutorul unui dispozitiv electronic. Prin urmare putem afirma că astfel de probe au caracter latent în același sens în care îl au și amprentele digitale sau ADN -ul (acid dezoxiribonucleic). Pentru *a vedea* astfel de dovezi avem nevoie de echipamente și software specializat pentru că sunt *fragile*: pot fi modificate, deteriorate, distruse.

Nu trebuie să uităm că probele digitale pot să conțină la rândul lor probe fizice: ADN, amprente digitale, etc. Prin urmare, probele fizice trebuie protejate pentru a fi examinate în mod corespunzător.

[1] http://www.nw3c.org/
[2] http://www2.fbi.gov/hq/lab/org/cart.htm
[3] http://www.ioce.org
[4] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp

1.2 Terminologie

În ciuda anilor care s-au scurs de la conştientizarea importanţei acestui domeniu, la ora actuală nu există un punct de vedere comun cu privire la termenii folosiți. Nevoia de standardizare este acută cu atât mai mult cu cât în limba română nu au fost preluate toate accepțiunile sintagmei *„computer crime”*.

Etimologic, englezescul *„crime”* are înțelesul de crimă, delict, nelegiuire, asasinat, ucidere. „Computer crime” se referă la un set limitat de delicte definite de legislația americană în *Computer Fraud and Abuse Act*[5] iar de către legislația Marii Britanii în UK Computer Misuse Act[6].

Legislația din România reglementează infracțiunile informatice prin *Titlul III (Prevenirea şi combaterea criminalității informatice) din Legea 161 din 19/04/2003 privind unele masuri pentru asigurarea transparentei in exercitarea demnităților publice, a funcțiilor publice si in mediul de afaceri, prevenirea si sancționarea corupției* - publicată in Monitorul Oficial, Partea I nr. 279 din 21/04/2003.

Considerăm că exprimarea din limba română este o traducere mai puțin reuşită a englezescului *„computer crime”*. Întărim cele afirmate prin aducerea în atenție a altor sintagme de natură juridică din limba engleză: *„criminal procedure”, „Title 18 of the United States Code is the criminal and penal code of the federal government of the United States. It deals with federal crimes and criminal procedure”, „criminal law and civil law*” cu înțelesul „**legea penală şi legea civilă**”.

În contextul dat, „crime” are semnificația de „infracțiune”. De fapt, chiar legiuitorul român afirmă în textul actului normativ menționat:

„Art. 34. - Prezentul titlu reglementează prevenirea si combaterea criminalității informatice, prin măsuri specifice de prevenire, descoperire şi sancționare a ***infracțiunilor*** *săvârşite prin intermediul sistemelor informatice, asigurându-se respectarea drepturilor omului si protecția datelor personale.*”

În prezenta lucrare, „computer crime” va semnifica „*infracțiune informatică*”. Pornind de aici, considerăm că unul din cele mai dificile aspecte ce ține de definirea conceptului se referă la situațiile practice în care un calculator sau o rețea de calculatoare nu au fost implicate în mod direct în săvârşirea unei infracțiuni, dar conțin probe cu privire la săvârşirea infracțiunii. Pentru astfel de situații, literatura şi legislația anglosaxonă folosesc sintagma „*computer related*”, în timp ce Convenția Europeană referențiază termenul general „*cybercrime*”.

A doua sintagmă ce necesită standardizare este „*computer forensic*”, care în accepțiunea noastră are semnificația de „*investigații informatice*”. În literatura de specialitate vom întâlni şi cea de a doua exprimare „*digital forensic*”. Inițial cele două sintagme aveau acelaşi înțeles dar între timp „digital forensic” are în vedere toate dispozitivele capabile să stocheze date în format digital, nu doar calculatoarele. O definire în limba română a sintagmei „computer forensic” poate fi de forma:

Utilizarea de metode ştiințifice cu privire la conservarea, identificarea, extragerea, interpretarea, documentarea şi prezentare a probelor de natură digitală obținute din surse de natură informatică în scopul facilitării descoperirii adevărului şi furnizarea de expertiză în cadrul unui proces penal sau a unei proceduri administrative.[7]

La nivel internațional există diverse standarde şi instituții de standardizare precum Instituția de Standardizare Britanică şi Organizația Internațională asupra Probelor Digitale. Țări dezvoltate

5 http://itlaw.wikia.com/wiki/Computer_Fraud_and_Abuse_Act
6 http://www.legislation.gov.uk/ukpga/1990/18/contents
7 Traducere şi adaptare după definiția dată de Cyber Security Institute

din punct de vedere al gradului de informatizare precum SUA, Marea Britanie, Germania şi altele au adoptat aceste standarde care sunt mai mult un cadru de lucru sugerat decât nişte reguli stricte.

În România nu există nici o lege sau document oficial care să sugereze aderarea la aceste standarde internaţionale. Codul de procedură penală precizează că analiza echipamentelor care ar putea conţine informaţii care să incrimineze un suspect trebuie analizate de un specialist dar nu impune un anumit cadru de lucru. Alte referinţe la infracţionalitatea informatică mai pot fi găsite şi în Legea 161 din 19/04/2003 dar, la fel ca şi Codul de procedură penală, legea este incompletă şi nu acoperă toate aspectele infracţiunilor informatice.

1.3 Rolul calculatoarelor în realizarea infracţiunilor

Fără a intra prea mult în detalii, în paragrafele anterioare am căutat să evidenţiem importanţa limbajului într-un astfel de domeniu. Pentru practica autohtonă, rolurile pe care le poate juca calculatorul şi infrastructura de comunicaţii le regăsim în *SECTIUNEA a 2-a - Infracţiuni informatice* din actul normativ menţionat anterior. Exprimarea din actul normative nu ajută însă la clarificarea domeniului.

Pentru a înţelege cum poate fi utilizat un calculator (luat în ansamblul său) ca probă a unei infracţiuni trebuie înţeles exact rolul pe care acesta îl poate juca la un moment dat. Aceasta deoarece în literatura de specialitate, unii autori fac distincţie între probele electronice (aparţin componentelor hardware) şi probele digitale (informaţiile conţinute).

Deoarece legislaţia noastră nu dă dovadă nici de coerenţă nici de completitudine pentru acest subiect, afirmaţiile din continuarea acestei lucrări nu vor aborda subiectul strict din punct de vedere juridic, ci mai mult din perspectiva practicilor internaţionale. Aşa stând lucrurile spunem că există situaţii în care calculatorul dintr-o ţară poate fi folosit pentru a ataca un calculator dintr-o altă ţară iar victima infracţiunii să fie din a treia ţară!

Calculatorul poate fi deci identificat în următoarele ipostaze:

- *ţinta sau victima infracţiunii*
- *instrumentul prin care s-a realizat infracţiunea*
- *depozitarul probelor legate de o infracţiune.*

Un calculator sau o reţea de calculatoare poate fi oricând, virtual, victima unei infracţiuni. Avem în vedere aici sabotajul, furtul sau distrugerea informaţiilor stocate în memoria sa. În acest caz sunt vizate cele trei caracteristici fundamentale ale securităţii echipamentului: *confidenţialitatea, integritatea* sau *disponibilitatea*. Un exemplu relativ recent în acest sens îl reprezintă atacurile la adresa siturilor VISA şi Mastercard în urma arestării deţinătorului WikiLeaks, Julian Asange. Atacurile cu ajutorul viruşilor informatici pot fi încadrate tot în acest tip.

Calculatorul poate fi folosit însă şi ca o *armă* pentru realizarea unor tranzacţii financiare frauduloase, încălcarea drepturilor de proprietate intelectuală, realizarea de falsuri (falsul privind identitatea, de exemplu). În acest caz putem spune că infracţiunile sunt în fapt *ajutate* de către calculator.

Ultimul rol, cel de *martor* al infracţiunii este unul oarecum duplicitar pentru că această situaţie se regăseşte în oricare din variantele anterioare. Calculatorul este cel care poate ajuta la identificarea informaţiilor folosite în săvârşirea unei infracţiuni.

Această distincţie a rolurilor, între subiect sau obiect al infracţiunii, ajută cel mai bine investigatorul pentru că în fapt evidenţiază intenţia celui care a săvârşit infracţiunea. În practică însă sunt rare situaţiile în care o infracţiune poate fi încadrată într-o singură categorie datorită modului în car tehnologiile au fost concepute şi funcţionează.

Capitolul 2. Proba digitală

Mărturia sau demonstraţia unui fapt stă la baza dovezii juridice: o amprentă, o pată de sânge sau ceea ce în literatura de specialitate americană se numeşte „smoking gun" (en: armă cu care abia s-a tras). În continuare vom demonstra că proba digitală se încadrează în acest peisaj.

2.1 Proba digitală - definiţie

Potrivit Merriam-Webster's Dictionary of Law, cuvântul probă[8] (en: evidence) înseamnă *ceva care furnizează sau poate furniza dovezi; ceva care este predat în mod legal unui tribunal pentru a se afla adevărul despre un anumit lucru*.

În 1998, un grup de organizaţii angajate activ în domeniul probelor digitale, pentru a promova comunicarea şi cooperarea, precum şi asigurarea calităţii şi coerenţei în cadrul comunităţii investigaţiilor digitale, sub denumirea de The Scientific Working Group on Digital Evidence (SWGDE)[9] au definit termenul probă digitală ca *„orice informaţie cu valoare probativă care este stocată sau transmisă în format electronic*".

După cum a fost testat şi definit în diverse instanţe din SUA, probele digitale sunt dovezi generate, stocate sau transmise în format electronic. Aceste dovezi pot rezida în telefoane mobile, pagere, asistent personal digital (PDA) sau calculator. Teoretic, deci, o probă digitală rezidă în orice echipament care poate fi utilizat în transmiterea şi stocarea informaţiilor în format binar (mesaje text sau SMS, e-mail-uri, baze de date sau log-uri de pe servere cu precădere Web).

Probele digitale sunt utile în cazuri minore de urmărire a unei persoane pe Internet dar, devin critice, în cazuri de piraterie şi spionaj industrial. Cel mai frecvent, se face uz de astfel de probe digitale în mediul economic, anchetarea unor angajaţi cu privire la activităţi ilegale desfăşurate în timpul serviciului sau breşe de securitate în reţelele corporaţiilor. Având în vedere sumele de bani tranzacţionate în mediul economic, aceste aspecte nu vin ca o surpriză. Cele mai întâlnite astfel de situaţii sunt cauzate de angajaţi care folosesc echipamentele informatice ale organizaţiei în scopuri personale, navigarea pe Internet pe site-uri cu conţinut pornografic, download sau/şi distribuţie de software fără licenţă. Breşele de securitate pot avea originea în surse externe companiei precum o persoană cu intenţia de a exploata anumite vulnerabilităţi ale reţelei pentru a sustrage sau şterge informaţii sensibile sau surse interne caz în care un angajat încearcă să obţină informaţii peste nivelul său de acces.

2.2 Standarde internaţionale

Instituţia de Standardizare Britanică (British Standard Institution (BSI)) [10] a publicat o serie de proceduri şi recomandări care să asigure un minim de valoare unei probe digitale pentru a fi recunoscută şi acceptată ca probă într-un proces. Standardele au căpătat recunoaştere internaţională şi acoperă modul corespunzător de manipulare şi păstrare a probelor digitale, de la creare sau descoperire de către anchetatori până la folosirea efectivă într-un caz de judecată. Cuvântul cheie este audit sau, mai precis, metode pentru a oferi răspundere, autenticitate (certificare) şi non-

[8] http://www.merriam-webster.com/dictionary/evidence?show=0&t=1305015887
[9] http://www.swgde.org/about-us/
[10] http://www.bsigroup.com/ accesat la 10/05/2011 ora 11:57

repudiere a înregistrărilor, astfel încât să fie admisibile ca mijloc de probă. Acestea sunt similare cu standardele din Statele Unite.

Organizația Internațională asupra Probelor Digitale (International Organization on Computer Evidence (IOCE)) a fost înființată în anul 1995 pentru a oferi agențiilor internaționale de aplicare a legii un forum pentru schimbul de informații privind criminalitatea informatică. Compus din agențiile guvernamentale acreditate implicate în investigații asupra infracționalității informatice, IOCE identifică și discută problemele de interes a elementelor sale constitutive, facilitează difuzarea internațională de informații, dezvoltă recomandări în vederea examinării de către agențiile membre. În plus față de formularea normelor de lucru cu probe digitale, IOCE ține conferințe orientate spre stabilirea de relații de muncă.

Ca răspuns la Comunicatul și planurile de acțiune al G-8 din 1997[11], IOCE a fost însărcinată cu dezvoltarea standardelor internaționale pentru schimbul și recuperarea probelor digitale. Grupurile de lucru în Canada, Europa, Marea Britanie, și Statele Unite au fost formate pentru a aborda această standardizare.

În timpul conferinței *Hi-Tech Crime and Forensics Conference (IHCFC)* din octombrie 1999, IOCE a ținut întâlniri și un workshop care a revizuit Ghidul de bune practici al Marii Britanii și Proiectele de standarde ale SWGDE. Grupul de lucru a propus următoarele principii, care au fost votate de către delegațiile IOCE cu aprobare unanimă:

- Coerența cu toate sistemele juridice;
- Utilizarea unui limbaj comun;
- Durabilitate;
- Abilitatea de a insufla încredere în integritatea probelor;
- Aplicabilitatea la toate probele digitale;
- Aplicabilitate la fiecare nivel, individ, agenție, țară.[12]

2.3 Păstrarea probelor digitale

Pentru a prezenta probele digitale ele trebuie mai întâi examinate. Înaintea examinării acestea trebuiesc stocate. Cum sunt identificate, colectate şi manipulate probele sunt cele mai importante informaţii dintr-o astfel de prezentare. Pentru a putea fi considerată admisibilă într-un proces, trebuie demonstrat că proba digitală este relevantă şi „materială". Orice urmă de dubiu asupra integrităţii probei şi asupra modului de manipulare o fac inutilă.

Când ne gândim la păstrarea unei probe digitale ar trebui să ne gândim la modul cum se face conservarea locului unei investigaţii criminalistice obişnuită. Trebuie documentat fiecare detaliu, trebuie făcute poze şi jurnalizată cât mai multă informaţie posibilă asupra stării în care a fost găsită proba şi bineînţeles a modului care a dus la descoperirea ei. Trebuie menţionat aici că dacă probele se află pe un calculator care funcţionează la momentul descoperirii, trebuie acţionat cu deosebită prudenţă deoarece se pot pierde foarte uşor datele volatile.

În continuare abordăm activităţile cheie în investigarea locului unei infracţiuni digitale pentru a asigura relevanţa şi „materialitatea" probei digitale.

2.4 Lanţul de custodie

Regula principală când suntem în procesul de colectare, manipulare şi în general lucrul cu probe digitale este aceea de a documenta tot ce se întâmplă.

Standardele internaţionale recomandă ca lanţul de custodie să fie unul din cele mai importante documente care trebuie să se regăsească în „trusa" unui investigator. În cazul în care integritatea unei probe digitale este pusă la îndoială, acest document oferă o imagine clară asupra

[11] http://www.justice.gov/criminal/cybercrime/g82004/97Communique.pdf
[12] Adaptat după http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

tuturor persoanelor care au avut acces la probe. Dacă se ajunge la tribunal, lanţul de custodie este primul lucru care este pus la îndoială de apărarea acuzatului.

Lanţul de custodie este un document scris care descrie în amănunt modul în care probele au fost identificate, colectate, stocate şi manipulate, de cine, când şi în ce scop. Potrivit documentului RFC 3227, "Guidelines for Evidence Collection and Handling,"[13] al organizaţiei IETF[14] (The Internet Engineering Task Force), lanţul de custodie ar trebui să furnizeze următoarele:

- Unde,când şi de către cine au fost descoperite şi colectate probele digitale;
- Unde, când şi de către cine au fost examinate şi manipulate probele digitale;
- Cine a avut posesia probelor digitale, cum au fost stocate şi când;
- Când au fost schimbaţi posesorii probelor, de ce şi când , unde şi cum a avut loc schimbul;
- Descrierea fizică a echipamentului pe care sunt păstrate probele digitale (producător, model, SN, mărimea unităţii, etc.);
- Valorile Hash, dacă este cazul.

Exemplu de Jurnal de evidenţă a custodiei:

Descriere probă/număr	**Data achiziţie**	**Locul achiziţiei**	**Metoda achiziţiei**	**Achiziţionat de la**	**Semnătura**	**Locul stocării**
	Data transferării	**Transferat la**	**Motivul transferării**	**Aflat actual în custodia**	**Semnătura**	**Locul stocării**

Informaţii suplimentare: _____

2.5 Probe volatile vs. probe nevolatile

Volatilitatea sursei unei probe digitale este primul lucru care trebuie luat în considerare când colectăm, asigurăm şi examinăm o astfel de probă. Termenul volatilitate, în acest context, înseamnă „susceptibil schimbării". Cu alte cuvinte, integritatea şi disponibilitatea unei probe digitale pot fi foarte uşor compromise sau proba poate fi distrusă.

O acţiune simplă precum închiderea echipamentului suspect sau oprirea/pornirea alimentării cu energie electrică poate pune în primejdie informaţii potenţial valoroase care rezidă în memoria RAM; fişiere pe jumătate terminate sau nesalvate, fişiere deschise, e-mailuri, parole, nume de utilizator, adrese Web şi piese de program maliţios. Trebuie ştiut că unele programe rulează doar în memoria RAM pentru a evita detecţia în cazul unei examinări a hard disk-ului. Aceste informaţii sunt irecuperabile atunci când calculatorul sau echipamentul este închis sau se întrerupe alimentarea cu energie electrică. Adiţional se pierd informaţii precum procesele ce rulează la momentul respectiv, informaţii din zona de swap sau pagefile precum şi informaţii despre reţea. De aceea aceste informaţii sunt clasificate ca volatile.

Probele digitale non-volatile se referă la date sau informaţii care deşi sunt susceptibile schimbării (ex: data ultimei accesări, informaţii despre utilizator), înţelesul şi conţinutul principal care constituie dovada nu se pierd. Datele din document rămân aceleaşi indiferent de starea

[13] http://www.faqs.org/rfcs/rfc3227.html
[14] http://www.ietf.org/

echipamentului suspect (închis sau deschis, conectat sau nu la reţea/Internet). Aceste informaţii se referă în general la cele stocate pe hard disk-uri, medii portabile precum unităţi de stocare USB, dischete floppy, CD-uri şi DVD-uri, etc.

Ordinea general acceptată a volatilităţii probelor digitale, de la cele mai volatile la cele non-volatile este prezentată în figura 1.

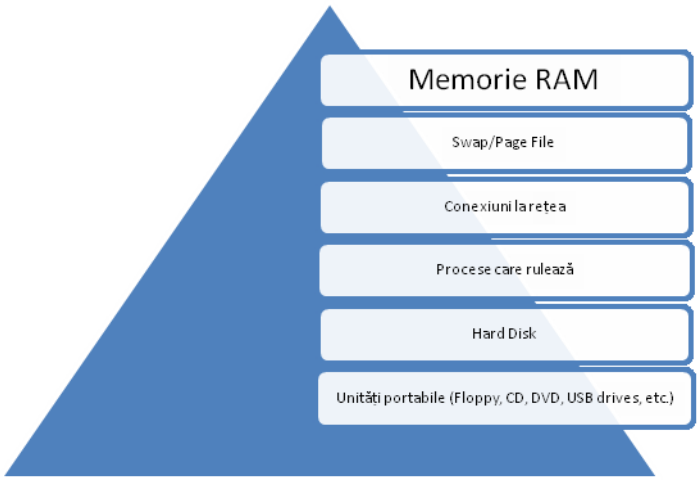


Figura nr. 2.1 – *Volatilitatea probelor digitale*[15]

Validarea şi examinarea probelor digitale volatile cât şi nevolatile ajută la scrierea „poveştii" probei la momentul colectării. În cazul codului maliţios care rulează strict în memorie „povestea" este spusă în întregime de memoria RAM.

2.6 Manipularea probelor digitale

Strângerea şi stocarea probelor digitale ar trebui documentate cu claritate dacă dorim să avem succes şi să câştigăm cazul. Cu cât este mai consistentă şi completă descrierea modalităţii de colectare, cu atât proba digitală va fi mai credibilă.

După cum am văzut şi mai sus, cea mai importantă regulă este documentarea fiecărei acţiuni. Fie că examinatorul sau investigatorul ţine un jurnal de mână sau un fişier electronic, este imperativ ca acest document să existe şi să ateste totul de la primul contact al investigatorului cu cel care cere investigarea şi cu proba până la prezentarea acesteia şi distrugere sau arhivare. Acest document este similar cu lanţul de custodie, principala diferenţă fiind asemănarea cu un jurnal de examinare, paşi şi proceduri urmate. Elementele cheie ale acestui document sunt:

- Data şi timpul fiecărui contact cu probele digitale (atât la începutul cât şi sfârşitul operaţiunilor);
- Numele examinatorului şi denumirea companiei pentru care lucrează;
- Descriere detaliată a echipamentului pe care se află proba digitală, tip, producător, model, număr de identificare şi fotografii;
- Descriere detaliată pentru fiecare acţiune la care este supusă proba digitală şi echipamentul în care este stocată;
- Data, timpul şi locul unde au fost depozitate echipamentele şi probele digitale după tragerea concluziilor (se recomandă un loc sigur cu seif protejat de apă, foc şi alţi factori de risc).[16]

[15] Adaptat după Handbook of Information Security, Volume 2, Hossein Bidgoli, pagina 660

Valoarea unei probe digitale este dată de modul cum "supravieţuieşte" contestaţiilor. Pentru aceasta trebuie dovedit că se află exact în aceeaşi stare în care a fost găsită şi colectată. Cea mai utilizată metodă de a oferi o astfel de certitudine este o sumă de control precum MD5 sau SHA-1. O astfel de sumă de control calculează o valoare unică numită "hash" care este echivalentul unei amprente în identificarea unei persoane. Valoarea hash este reprezentată de o valoare hexazecimală de 16 caractere calculată pe baza conţinutului unui fişier sau a unui disc. Odată ce valoarea hash originală a fost calculată, de fiecare dată când se va folosi o metoda de calcul asupra probei respective ea trebuie să fie identică. Acest lucru este posibil doar dacă proba nu a fost modificată. Chiar şi o operaţiune minoră precum deschiderea unui fişier pe un calculator cu sistem de operare Windows Windows ne poate compromite valoarea hash. În momentul în care deschidem documentul se schimbă cel puţin data şi timpul ultimei accesări rezultând o valoare hash nouă.

Orice probă digitală poate fi identificată unic de această valoare hash chiar şi cele volatile. Probele volatile trebuie colectate pe medii în format "write-once/read many", adică proba originală este scrisă pe un CD, de exemplu, care nu mai poate fi alterat decât prin compromitere fizică. Ca un ultim pas al colectării ar trebui să se calculeze o valoare hash a discului care mai apoi va fi notată în lanţul de custodie.

Pentru a colecta şi salva corespunzător probele non-volatile este nevoie de un alt procedeu şi anume copierea la nivel de bit (bit-level copy) a hard disk-ului. Acest lucru poate fi realizat atât cu software comercial dar şi freeware. Această metodă este superioară unei simple copieri deoarece informaţiile de pe un hard disk sunt duplicate la nivel de bit ceea ce înseamnă că sunt identice cu cele originale. Copierea simplă va schimba data şi timpul de pe documentul respectiv lucru care poate fi reflectat cu valoarea hash.

Pentru a ne asigura că probele sunt în siguranţă şi nu vor fi modificate, examinarea acestora se va realiza pe o copie la nivel de bit. Originalul trebuie păstrat într-un container protejat de energie statică şi alte intemperii, un seif la care se aibă acces cât mai puţini oameni posibil iar fiecare acces la seif trebui documentat riguros.

Prezentarea probelor digitale este probabil partea cea mai uşoară etapă a întregului proces. La început sunt prezentate probele fizice hard disk-uri, carduri de memorie, CD-uri, etc. Înregistrările din timpul examinării, lanţul de custodie, rapoartele autogenerate disponibile cu softurile comerciale, log-uri (bash din Linux) sunt documentele care susţin cazul şi atestă că pe dovezile fizice arătate există dovezi care incriminează suspectul. Dacă aceste documente sunt bine realizate şi nu lasă loc de dubiu cu privire la modul de operare în găsirea, colectarea, analiza şi păstrarea probelor procesul este ca şi câştigat. Cuvintele cheie într-o astfel de prezentare sunt validare, autentificare si non-repudiere.

2.6 Ştergerea probelor digitale

După colectarea, analiza şi prezentarea probelor digitale apare întrebarea cât de mult trebuie păstrate în continuare. Când este normal să se distrugă probele digitale şi cum se face acest lucru?

Păstrarea probelor digitale este necesară în momentul în care preconizăm că în viitor acestea ne vor ajuta să demonstrăm de ce am avut nevoie de ele, rejudecarea unui caz etc.

În domeniul economic chiar dacă nu există un ordin judecătoresc care să impună aceasta, probele digitale trebuie păstrate. Dacă se consideră ca nu mai este nevoie de ele trebuie păstrate documente cu privire la cine a aprobat distrugerea acestora, de ce, cine le-a distrus efectiv, cum şi când. La nivelul companiilor ar trebui să existe politici de retenţie sau distrugere a probelor digitale.

Există două motive pentru care ar trebui să păstrăm probele digitale şi anume: respectarea reglementărilor şi litigii.

În America, Actul Sarbanes-Oxley (SOX, 2002), impune ca documentele, inclusiv cele digitale să fie păstrate pentru 7 ani. Pedeapsa pentru nerespectarea acestui lucru este de nu mai

[16] Adaptat după Handbook of Information Security, Volume 2, Hossein Bidgoli, pagina 660

puţin de 10 ani de închisoare pentru managementul companiei şi o amendă substanţială de 5 milioane de dolari.

În România, păstrarea documentelor este reglementată prin Legea contabilităţii nr. 82/1991 şi Norma metodologică din 14/12/2004 de întocmire şi utilizare a registrelor şi formularelor comune pe economie privind activitatea financiară şi contabilă.

Când vine vorba de litigii, companiile sunt obligate să păstreze documentele altfel pot fi învinovăţite de distrugerea probelor incriminatorii şi luare parte la litigii. În afară de reglementari ale statului, companiile ar trebui să aibă propriile politici de păstrare a documentelor, inclusiv cele digitale şi revizuirea acestora ar trebui să fie un rol important pentru auditul intern.

Distrugerea documentelor electronice nu e aşa simplă precum a fost colectarea ei. Dacă ştergem un document de pe hard disk acesta nu a fost şters cu adevărat ci este marcat ca spaţiu liber peste care se pot scrie noi documente. Aşadar, pentru distrugerea probelor digitale avem două opţiuni şi anume rescrierea dispozitivului respectiv în întregime de câteva ori pentru a ne asigura că documentele vizate au fost "şterse" prin suprascriere şi cea de a doua variantă, distrugerea fizică a dispozitivului de stocare.

Există multe programe software care pot rescrie dispozitive de stocare. Un "best practice" este considerat rescrierea dispozitivului respectiv cu 0-uri şi 1 aleatorii pe toată suprafaţa acestuia de 3 ori. Departamentul de apărare SUA recomandă ca echipamentul sa fie 'şters' de 7 ori înainte de a fi dat spre re-utilizare.

Investigatorul trebuie să ia toate măsurile necesare pentru a colecta, păstra şi transporta probele digitale fără a le compromite:

- recunoaşterea, identificarea, sechestrarea şi securizarea probelor digitale la locul infracţiunii
- documentarea scenei infracţiunii şi a locului în care a fost identificată proba digitală
- colectarea, etichetarea şi conservarea probei digitale
- transportul securizat al probei digitale
- **nu se apasă nici o tastă şi nu se execută nici un clik de mouse.**

Capitolul 3. Dispozitive electronice: tipologie, descriere şi probe potențiale

Dispozitivele electronice însele şi informațiile conținute de acestea pot fi utilizate ca probe digitale.

3.1 Calculatoare

Un calculator este un ansamblu software şi hardware realizat cu scopul de a prelucra date şi poate să includă:

- o carcasă în care sunt încorporate placa de bază, procesorul, hard disk-ul, memoria internă şi diferite interfețe pentru conectarea altor echipamente periferice.
- monitor
- tastatură
- mouse
- periferice sau echipamente externe conectate.

Am folosit termenul generic de *calculator* dar vom înțelege în scopul acestui material şi laptop-urile/notebook-urile, sistemele instalate în stive, mini calculatoarele etc.

Figura nr. 3.1 – *Diferite tipuri de dispozitive de calcul*

Calculatorul şi toate componentele asociate sunt potențial probe digitale.

3.2 Dispozitive şi medii de stocare a datelor

Dispozitivele şi mediile de stocare a datelor din zilele de acum sunt mult mai diverse decât în urmă cu 5-10 ani. Tradițional, teoria grupează mediile de stocare în două mari categorii:

amovibile/detaşabile/mobile (floppy disks, CD-ROM, DVD, Zip disk, benzi magnetice, flash memory) respectiv non-amovibile (hard disk).

Din punct de vedere al tehnologiei utilizată pentru scrierea şi stocarea cele două categorii de medii de stocare folosesc fie scrierea optică fie scrierea magnetică.

Despre cele de mai sus am spus că sunt medii de stocare tradiționale. Deşi sunt încă folosite pe scară largă, încetul cu încetul au ajuns să fie înlocuite de dispozitivele USB, cardurile de memorie tip solid-state sau MP3 players. Toate aceste dispozitive pot fi folosite şi ca dispozitive de stocare a datelor, altele decât cele pentru care au fost inițial proiectate.

3.2.1 Hard Disk[17]

În cele mai multe cazuri, hard disk-urile reprezintă principala sursă de informații pentru un investigator. După cum spuneam încă din introducerea acestei cărți nu vom obosi cititorul cu prea multe detalii tehnice ci ne vom limita doar la acele informații necesare înțelegerii demersului investigativ. Pentru tehnicisme ... există oameni tehnici. În acest moment ne interesează mai mult modul de structurare a datelor pe aceste dispozitive.

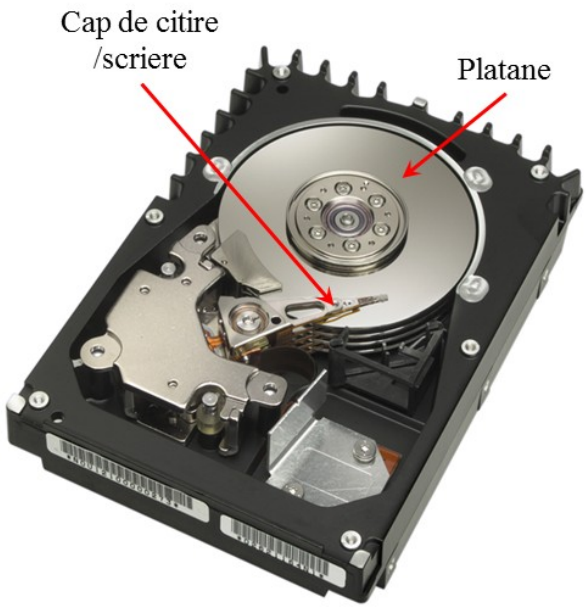


Figura nr. 3.2 - *Componentele interne ale unui hard disk*
(Sursa: http://www.hdd-tool.com/hdd-basic/hard-disk-and-hard-drive-physical-components.htm)

Din punctul de vedere al componentelor ne interesează:

- *geometria*: structura platanelor, pistelor şi sectoarelor
- *capul de citire/scriere*: elementul prin intermediul căruia informațiile sunt citite/scrise pe un hard disk. Există câte un cap pe fiecare platan
- *pistele/tracks*: sunt cercuri concentrice pe platanul unui disc. Datele sunt scrise pe piste

[17] O evoluț ie a acestor dispozitive este prezentată la adresa http://en.wikipedia.org/wiki/History_of_hard_disk_drives

- *cilindrii*: o coloană de piste de pe două sau mai multe platane. În mod normal, fiecare platan are două suprafețe
- *sectorul:* o secțiune de pe o pistă cu o dimensiune de 512 bytes.

Figura de mai jos sintetizează aceste informații.

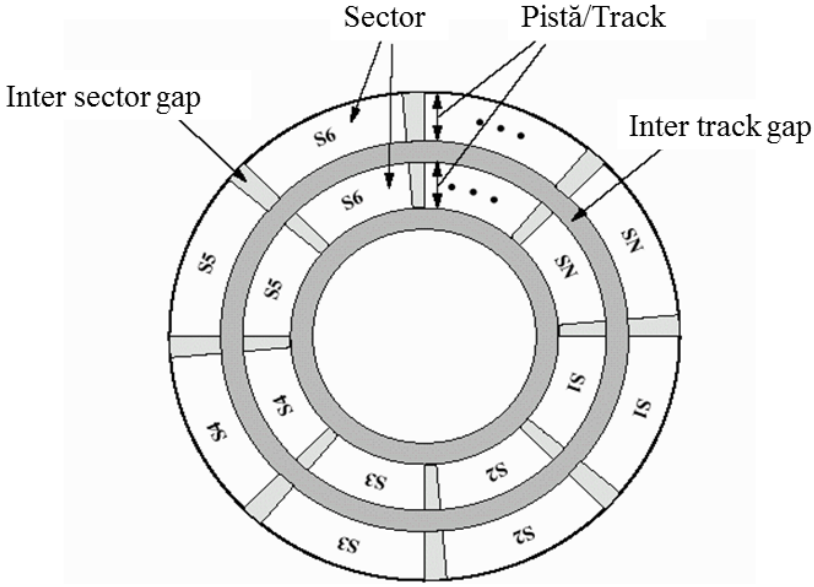


Figura nr. 3.3 – *Structura hard discului*
(Sursa: Adaptare după David Tarnoff Computer organization and design fundamentals Examining Computer Hardware from the Bottom to the Top, 2007)

Locul de amplasare şi numărul de sectoare de pe un disc sunt determinate şi scrise permanent de către producător prin intermediul low-level format. Zona dintre sectoarele de pe un hard disc se numeşte Intersector Gap.

Din punct de vedere al organizării logice, există un prefix ce conține numărul sectorului şi al pistei pentru a permite capului de citire/ scriere să determine localizarea fizică a acestor elemente precum şi existența unui bit deteriorat pentru a marca un sector ca inutilizabil în situația în care acesta devine imposibil de citit. Câmpul Sync este un model alternativ utilizat de către unitate pentru sincronizări. Câmpul Error Correcting Code (ECC) este adăugat de unitatea hardware pentru a detecta erorile la nivel de biți din datele stocate.

Hard discurile interne actuale (precum şi unitățile de bandă magnetică) se bazează pe două standarde de interfațare: SCSI (Small Computer System Interface)[18] şi SATA (Serial Advanced Technology Attachment). În cadrul acestor standarde de interfațare se întâlnesc mai multe generații tehnologice care reflectă evoluția în timp.

[18] Detalii la adresa http://www.scsilibrary.com/

Figura nr. 3.4 – *Tipuri de hardiscuri*

Figura nr. 3.5 – *Fişe de date pentru interconectarea hardiscurilor*

Pentru fiecare din aceste două standarde există aspecte specifice pe care investigatorul trebuie să le aibă în vedere.

În cazul SATA există posibilitatea securizării hard disk-ului cu ajutorul unei parole, distinctă de parola BIOS ce protejează calculatorul în momentul alimentării cu energie electrică. De obicei această facilitate este întâlnită în cazul hard disk-urilor laptop-urilor.

Chiar dacă nu este ştiută, parola de BIOS poate fi ocolită relativ simplu: se instalează hard diskul pe un alt calculator. În cazul SATA, parola este scrisă chiar pe hard disk, ne-parolată. Există două tipuri de astfel de parole: *user password* şi *master password*.

În cazul în care parola utilizator nu este disponibilă investigatorului, se poate căuta parola Master de la producătorul hard disk-ului, calculatorului sau compania care administrează calculatorul. Dacă acest lucru nu este posibil se achiziționează o soluție de deblocare a hard diskului şi se instalează împreună cu hard disk-ul inaccesibil pe un calculator funcționabil. Mai există şi posibilitatea aplicării unor tehnici de inginerie socială pentru a afla parola.

În ceea ce priveşte achiziția datelor de pe discuri SCSI, ori de câte ori este posibil, acest lucru trebuie realizat pe calculatorul original. Se impune o astfel de abordare ca efect al versiunilor de standard existente: (SCSI-1, SCSI-2, sau SCSI-3).

Mai există o situație: hard disk-urile externe. Din punct de vedere al conectării aceste hard disk-uri folosesc două standarde: USB (Universal Serial Bus) şi FireWire (IEEE 1394). Din această cauză este important ca investigatorul să aibă pe calculatorul său astfel de porturi.

Pentru a oferi toleranță în cazul unor evenimente neprevăzute, majoritatea serverelor folosesc hard diskuri configurate în sistem RAID - (Redundant Array of Inexpensive Disks). Sistemele de hard disk-uri RAID pot fi configurate cu ajutorul hardware (controller) sau software.

3.2.2. Banda magnetică

Acest dispozitiv de stocare este întâlnit mai ales ca suport pentru copiile de siguranță realizate pentru datele din producție ale unei organizații. În organizațiile ce aplică principiile

guvernării şi securităţii IT, copiile de siguranţă/benzile magnetice nu sunt păstrate în sediul principal ci într-un alt sediu/amplasament.

Când se confruntă cu acest tip de medii de stocare, un investigator trebuie să aibă în vedere trei aspecte: hardware, software şi capacitatea.

Din punct de vedere hardware, cele mai folosite tehnologii sunt: DLT (Digital Linear Tape), LTO (Linear Tape-Open), Exabyte, AIT (Advanced Intelligent Tape), DAT (Digital Audio Tape) şi QIC (Quarter inch cartridge)[19]. În plus, fiecare dintre aceste tehnologii vine într-o varietate de dimensiuni. O anumită unitate poate sau nu poate fi capabilă să citească versiuni mai vechi sau mai noi ale aceleiaşi tehnologii. Ca rezultat, este de o importanţă majoră ca dispozitivul de bandă să fie achiziţionat împreună cu tipul de benzi specifice.

Figura nr. 3.6 – *Banda magnetică*

Din punct de vedere software, majoritatea producătorilor de soluţii tip backup folosesc formate diferite pentru stocare datelor. În cazul Microsoft avem de a face cu MTF – Microsoft Tape Format. Ca efect al caracteristicilor fiecărui produs în parte, este posibil ca în cazul recuperării datelor de pe benzi magnetice să fie nevoie de software-ul producătorului respectivului dispozitiv.

Din punctul de vedere al capacităţii foarte mari de stocare, investigatorul trebuie să ţină cont că realizarea unei copii bit cu bit este aproape imposibilă în lipsa unui dispozitiv de stocare similar. Prin urmare investigatorul se va concentra în primul rând pe identificare fişierelor relevante pentru investigaţie.

3.2.3. CD şi DVD

Mediile optice prezintă trei formate de scriere a datelor: inscripţionabile o singură dată, reinscripţionabile şi „prin presare” (în cazul producţiei de masă). Nu este în scopul acestui material să intră în prea multe detalii tehnice cu privire la tehnologiile utilizate pentru fiecare caz în parte.

Microsoft foloseşte CDFS - CD File System, o versiune a standardului ISO 9660 pentru stocarea optică a datelor. Investigatorul trebuie să ştie că există o limită de 32 de caractere pentru numele fişierelor, dincolo de care numele va fi trunchiat. În aceste situaţii este nevoie de o analiză a fişierelor pentru a identifica mai întâi conţinutul care face scopul investigaţiei.

În cazul DVD-urilor se foloseşte Universal Disk Format (UDF), un standard ce oferă suport atât pentru numele lungi de fişiere cât şi pentru caracterele Unicode.

[19] Pentru detalii *www.exabyte.com/support/online/documentation/whitepapers/history.pdf*

3.2.4. USB/Flash Drive, Memory Card

Dispozitivele de memorare tip flash sunt un lucru comun în aceste zile. La bază ele folosesc memoria EEPROM - Electrically Erasable, Programmable Readonly Memory. Spre deosebire de hard disk-uri, acest tip de memorie oferă viteze mai mari de citire scriere, dimensiuni reduse şi o densitate de stocare mai mare.

De la ceasuri la MP3 playere, memoriile tip USB/flash îmbracă o multitudine de forme: CompactFlash, Smart Media, Memory Sticks.

Figura nr. 3.7 – *Diferite tipuri de unități de stocare a datelor*

La început, capacitatea de stocare a USB flash drive-urilor era redusă. Astăzi, datorită evoluțiilor tehnologice, aceste dispozitive nu mai sunt folosite doar pentru stocarea transferul fişierelor ci pot să conțină variante de sisteme de operare folosite pentru pornirea calculatoarelor.

În ultimul timp multe astfel de dispozitive sunt livrate cu capabilități de protejare a accesului prin parolă.

3.2.5. Dispozitive *handheld*

Sub această denumire generică sunt grupate acele echipamente ce oferă facilități de comunicare, fotografiere, GPS, divertisment on line, management de informații personale, stocarea datelor.

Le cunoaştem mai curând sub denumirea de „smart phone”.

În cazul anumitor tipuri de telefoane mobile există posibilitatea ca de la distanță dispozitivul să poată fi făcut inutilizabil. Investigatorul trebuie să verifice acest aspect înainte de sechestrarea/confiscarea dispozitivului.

Capitolul 4. Fundamentele rețelelor de calculatoare

În perioada actuală, când aproape toate dispozitivele electronice au posibilitatea de interconectare la Internet, este aproape imposibil să tratăm domeniul investigațiilor informatice fără a aminti despre câteva aspecte legate de rețele de calculatoare.

Conceptul de *nivel* este folosit pentru a vă ajuta să înțelegeți acțiunile şi procesele ce apar în timpul transmiterii informațiilor de la un calculator la altul. Într-o rețea, comunicarea are la origine o sursă, apoi informația circulă până la o destinație. Informațiile care traversează rețeaua sunt referite ca *date*, *pachete* sau *pachete de date.*

Adresa sursă a unui pachet de date specifică identitatea calculatorului care transmite respectivul pachet. Adresa destinație precizează identitatea calculatorului care va recepționa pachetul. Datele sunt grupate în unități logice de informații. Ele includ utilizatorul respectivelor informații şi alte elemente pe baza cărora este posibilă comunicarea.

Datele dintr-un calculator sunt reprezentate prin biți. Dacă un calculator ar transmite doar unul sau doi biți, nu ar fi o manieră prea eficientă de comunicare. Prin urmare, are loc o grupare a acestora în kilo, mega sau gigabytes.

Am făcut deja referire la un alt element întâlnit în rețelele de calculatoare: „*mediul*". Acesta reprezintă un material prin care sunt transmise datele, şi poate fi unul din următoarele elemente:

- cablu telefonic;
- cablu UTP;
- cablu coaxial (cablu TV);
- fibră optică;
- alte tipuri de cabluri bazate pe cupru

Mai există şi alte tipuri de media. În primul rând este vorba de atmosfera prin care se propagă undele radio, microundele şi lumina. În al doilea rând este vorba de undele electromagnetice care traversează Cosmosul, unde în mod virtual nu există molecule sau atomi. În aceste cazuri, comunicația este denumită *fără fir.*

Protocolul reprezintă un *set de reguli pe baza căruia se determină forma datelor şi transmisia acestora.* Exemplu lui Andrew Tanenbaum[20] (comunicarea între doi filosofi) este un început bun pentru a înțelege ce presupune comunicarea bazată pe niveluri şi protocoale (fig. 1.3.1.).

Nivelul *n* al unui calculator poate comunica cu nivelul *n* al altuia, nu direct ci prin intermediul nivelului inferior. Prin urmare se spune că regulile folosite în comunicare se numesc *protocoale de nivel n*.

[20] Adaptare după Andrew S. Tanenbaum: "Retele de calculatoare", Editia a treia, Editura Agora, Tg. Mures, 1998, pg. 18

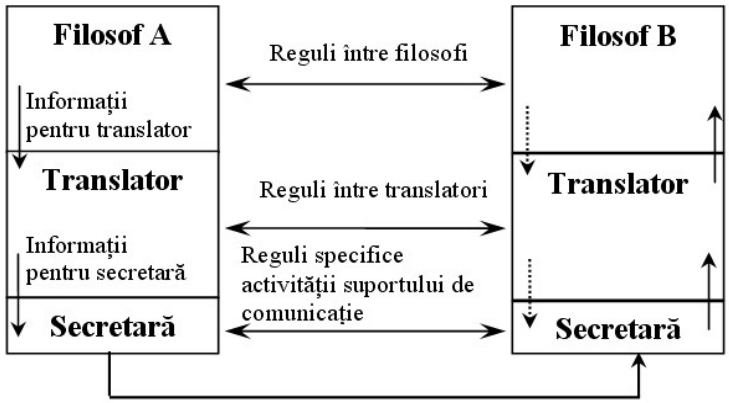


Figura nr. 4.1 - *Modelul de comunicare între filosofi*

Un alt exemplu pentru explicarea transferului între două calculatoare este modul în care putem citi o pagină web aflată pe un calculator situat la mare distanță:

- utilizatorul lansează un program pentru vizualizarea paginilor web (browser);
- browserul este entitatea aplicație care va „negocia" pentru noi obținerea paginii;
- nivelul aplicație va identifica existența resursei cerute de client (clientul este browserul, care-l reprezintă pe utilizator în această „tranzacție") şi a posesorului acestea (serverul – înțeles ca fiind entitatea ce oferă resursa cerută, nu calculatorul central al unei rețele; în cazul nostru, avem de-a face cu un server de web). Se realizează autentificarea serverului (se verifică dacă partenerul este într-adevăr cine pretinde că este şi se stabileşte dacă acesta este disponibil);
- nivelul sesiune va stabili o conexiune între procesul client şi procesul server;
- nivelul transport se va ocupa de întreținerea conexiunii şi de corectarea erorilor netratate la nivelul rețea;
- nivelul rețea va asigura transferul datelor în secvențe (pachete), stabilind drumul acestora între server şi client.

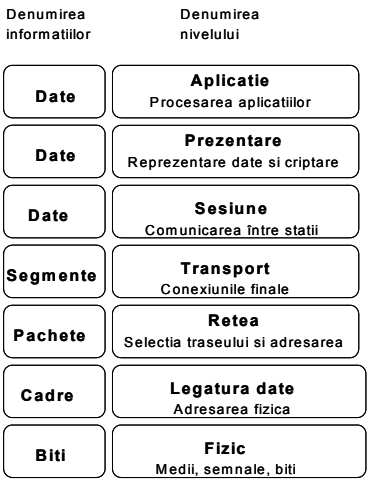
4.1 Modelul OSI

Lucrurile sunt ceva mai complicate decât în cele prezentate mai sus. Datele sosesc prin intermediul mediului de comunicație ca un flux de biți. La nivelul legăturii de date, biții sunt transformați în cadre, iar la nivelul rețea în pachete (vom vedea mai târziu cum arată un pachet). În cele din urmă, datele ajung la nivelul aplicație unde sunt preluate de browser şi ne sunt prezentate. Fiecare nivel adaugă sau şterge o parte din informațiile de control ataşate datelor de celelalte niveluri.

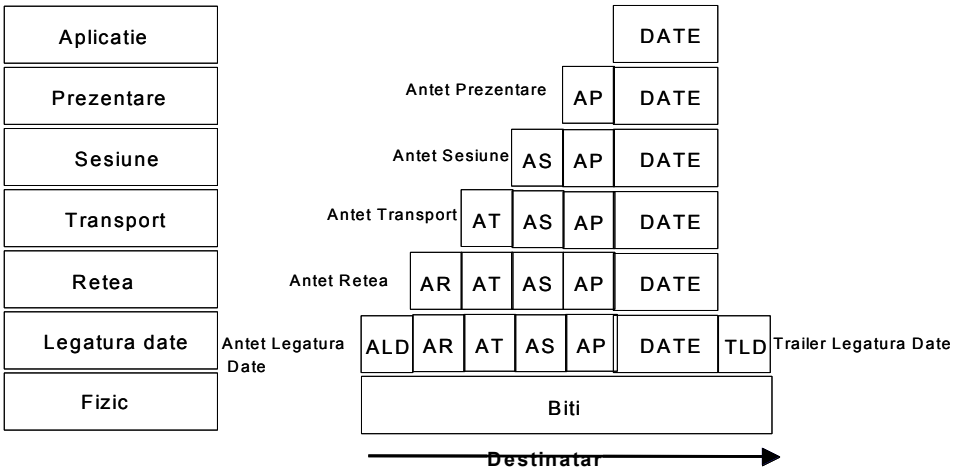
Spuneam că dezvoltările timpurii din zona rețelelor au fost haotice, şi că începutul anilor '80 se caracterizează printr-o expansiune a acestora. Singura modalitate prin care deținătorii de rețele puteau să "vorbească aceeaşi limbă" a fost agrearea din partea vânzătorilor şi producătorilor de echipamente de rețea a unui set comun de standarde.

International Organization for Standardization (*ISO*) este organizația care a cercetat şi dezvoltat scheme de rețele precum DECNET, SNA, TCP/IP. Rezultatul cercetărilor s-a concretizat într-un model de rețea care i-a ajutat pe producători să creeze echipamente compatibile între ele.

Modelul de referință OSI (Open Systems Interconnect), realizat în 1984, nu este altceva decât o schemă descriptivă care a pus la dispoziția vânzătorilor standardele necesare asigurării compatibilității şi interoperabilității între diferitele tehnologii. Şi este cel mai bun instrument pentru învățare.



Modelul de referință OSI, este primul model pentru standardizarea comunicațiilor în rețele. Există şi alte modele, dar majoritatea producătorilor de echipamente respectă aceste standarde. Acest model permite utilizatorilor să vadă funcțiile rețelei pe măsură ce ele apar la fiecare nivel în parte. Chiar dacă pare destul de abstract, este un instrument foarte bun pentru a ilustra modul în care informațiile traversează o rețea: explică vizual circulația datelor de la o aplicație, către mediul fizic de transmisie şi apoi către o altă aplicație localizată pe un calculator din rețea, chiar dacă expeditorul şi destinatarul fac parte din rețele cu topologii diferite. După cum se vede şi din figura alăturată, în modelul de referință OSI există 7 niveluri, fiecare dintre acestea ilustrând o funcție particulară a rețelei. Separarea între funcțiile rețelei este denumită *nivelare (layering)*.



Când aplicația de pe calculatorul sursă transmite, datele sunt grupate sub forma *pachetelor* ce traversează în jos nivelurile inferioare. La nivel fizic, biți sunt convertiți sub forma de impuls electric, undă radio sau lumină. La destinație, datele suferă un proces invers până la nivelul aplicație. Pe măsură ce datele traversează în jos cele 7 niveluri, primesc informații suplimentare (antete sau trailere). În timpul *încapsulării*, datele din pachet nu sunt modificate.

Modelul OSI este doar un model de arhitectură de rețea, deoarece spune numai ceea ce ar trebui să facă fiecare nivel, dar nu specifică serviciile şi protocoalele utilizate la fiecare nivel. Fiecare nivel al modelului OSI are un set predeterminat de funcții pe care le realizează pentru a duce la bun sfârşit comunicarea.

Nivelul 1: Fizic

Acest prim nivel îndeplineşte sarcinile cerute de nivelul legătură date şi vizează componentele hardware din rețea, specificațiile electrice, mediile de transmisie. Altfel spus se ocupă mai mult de parte electrică/electronică a comunicației principalele sale sarcini fiind:

- inițierea şi finalizarea conexiunilor către mediul fizic de transmisie;
- participă la controlul fluxului de date transmise pe un mediu;
- conversia datelor din formatul digital în semnale transmise pe un mediu.

Putem face o analogie între acces nivel şi instrumentele de lucru din procesorul de texte WORD: diferite formate de pagină, diferite tipuri de fonturi, culori diferite pentru fonturi etc.

Nivelul 2: Legătură date

Este nivelul care asigură mecanismele procedurale şi funcţionale prin care se transmit datele între nodurile unei reţele prin tranzitarea lor de la nivelul fizic pe baza adresării fizice, topologiei reţelei, notificării erorilor, ordonarea cardurilor şi controlul fluxului informaţional. Gândiţi-vă la controlul accesului pe un aeroport.

Nivelul 3: Reţea

Este unul dintre cele mai complexe niveluri; asigură conectivitatea şi selecţia căilor de comunicaţie între două sisteme ce pot fi localizate în zone geografice diferite. Principala sa sarcină o reprezintă transmiterea informaţiilor de la calculatorul sursă către calculatorul destinatar. Pentru a rezolva această problemă, nivelul reţea este cel care va selecta şi traseul pe care vor fi transportate informaţiile, indiferent de lungimea lor. Poate fi asemuit cu mecanismul prin care sunt dirijate trenurile într-o gară.

Nivelul 4: Transport

Este nivelul la care are loc segmentarea şi reasamblarea datelor. El furnizează un serviciu pentru transportul datelor către nivelurile superioare, şi în special caută să vadă cât de sigur este acesta. Nivelul transport oferă mecanisme prin care stabileşte, întreţine şi ordonă închiderea circuitelor virtuale; detectează "căderea" unui transport şi dispune refacerea acestuia; controlează fluxul de date pentru a preveni rescrierea acestora. Gândiţi-vă la calitatea serviciilor sau la încredere!

Nivelul 5: Sesiune

După cum spune chiar numele său, acest nivel stabileşte, gestionează şi finalizează sesiunile de comunicaţie între aplicaţii. Prin sesiune se înţelege dialogul între două sau mai multe staţii de lucru/echipamente de reţea. Nivelul sesiune sincronizează dialogul între nivelurile sesiune ale entităţilor şi gestionează schimbul de date între acestea. În plus, acest nivel oferă garanţii în ceea ce priveşte expedierea datelor, clase de servicii şi raportarea erorilor. În câteva cuvinte, acest nivel poate fi asemuit cu dialogul uman.

Nivelul 6: Prezentare

Este nivelul care asigură că informaţiile pe care nivelul aplicaţie al unui sistem le transmite, pot fi citite de către nivelul aplicaţie al altui sistem. Atunci când este necesar, nivelul aplicaţie face translaţie între diferitele formate ale datelor folosind un format comun pentru reprezentarea acestora. Trebuie să priviţi acest nivel ca cel la care are loc codificarea datelor în format ASCII, de exemplu.

Nivelul 7: Aplicaţie

Poetic vorbind, este nivelul situat cel mai aproape de inima utilizatorului. Prin ce diferă de celelalte niveluri ale modelului? Oferă servicii pentru aplicaţiile utilizatorilor dar nu oferă servicii celorlalte niveluri.

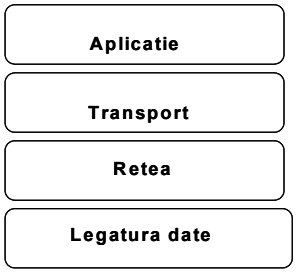
Nivelul aplicaţie identifică şi stabileşte disponibilitatea partenerului de comunicaţie, sincronizează aplicaţiile între ele şi stabileşte procedurile pentru controlul integrităţii datelor şi erorilor. De asemenea identifică dacă există suficiente resurse pentru a sprijini comunicaţia între parteneri. Pentru a fi mai uşor să vă amintiţi despre acest nivel, gândiţi-vă la telecomanda TV: o folosiţi dar nu ştiţi ce se întâmplă în interiorul său..

4.2 Modelul TCP/IP

Am început acest capitol cu modelul OSI deoarece reprezintă abecedarul acestui domeniu, fiind mai mult un instrument academic folosit pentru înțelegerea conceptelor folosite în domeniul comunicațiilor de date Cu toate acestea, pentru transmisiile de date din cea mai mare rețea existentă – Internetul, standardul folosit este *TCP/IP (Transport Control Protocol/Internet Protocol)*. Acest model a fost creat de Ministerul Apărării din SUA care a dorit să construiască o rețea capabilă să reziste în orice condiții, chiar şi într-un război nuclear. Era extrem de important să fie creată o rețea capabilă să opereze cu o infrastructură distrusă în proporție de peste 90%, fără să aibă vreo importanță starea fizică a anumitor segmente ale rețelei.

Astăzi, termenul generic „TCP/IP" cam tot ce are legătură cu protocoalele TCP şi IP.

Spre deosebire de OSI, modelul TCP/IP are doar patru niveluri: aplicație, transport, internet/inter-rețea şi legătură date. Deşi există niveluri cu acelaşi nume ca la modelul OSI, nu trebuie confundate cu acelea pentru că fiecare nivel are funcții total diferite.



Nivelul aplicație

Proiectanții TCP/IP au considerat că protocoalele de nivel înalt din acest model trebuie să includă detalii cu privire la sesiunile de lucru şi modul de prezentare a datelor. Astfel, într-un singur nivel sunt combinate toate facilitățile legate de reprezentarea datelor, codificare şi controlul dialogului.

Nivelul transport

Acest nivel vizează calitatea serviciilor oferite: încrederea în transmisie, controlul fluxului de date şi corectarea erorilor. Unul din protocoalele întâlnite la acest nivel (Transport Control Protocol), oferă o modalitate flexibilă de realizare a comunicațiilor în rețea. Fiind un protocol orientat conexiune, dialogul dintre sursă şi destinație se realizează prin împachetarea informațiilor de la acest nivel în segmente.

Orientarea către conexiune nu înseamnă că între calculatoarele care comunică există vreun circuit, ci că segmentele nivelului 4 circulă înainte şi înapoi între cele două calculatoare într-o perioadă de timp dată.

Nivelul internet/rețea

Scopul acestui nivel este de a trimite pachetele sursă din orice rețea către o alta, şi să facă astfel încât acestea să ajungă la destinație indiferent de ruta şi rețeaua din care au fost transmise. Protocolul care guvernează acest nivel este Internet Protocol, funcțiile îndeplinite de acesta fiind determinarea şi comutarea pachetelor (gândiți-vă la sistemul poştal).

Nivelul legătură date

Numele acestui nivel este cam general în cazul acestui model şi de multe ori creează confuzie. Este nivelul care include detalii despre tehnologiile LAN/WAN, precum şi toate detaliile incluse in nivelele fizic şi legătură date din modelul OSI.

De ce trebuie să învățați despre două modele când unul (cel mai adesea TCP/IP) ar fi suficient? Specialiştii preferă modelul OSI pentru analize mai atente şi ca fundament în orice discuție legată de rețele. Este adevărat că TCP/IP este mai folositor pentru că este implementat în lumea reala. Ca utilizatori finali aveți de-a face numai cu nivelul Aplicație, dar cunoaşterea detaliată a nivelurilor este vitală pentru realizarea unei rețele. Este adevărat că majoritatea utilizatorilor nu ştiu mai nimic despre protocoale de rutare sau alte detalii, dar este de asemenea adevărat că aceşti utilizatori nu trebuie să realizeze rețele scalabile şi sigure (şi nici nu au de dat examene la astfel de discipline).

Chiar dacă sunt voci care consideră drept imbecil modelul OSI, noi ne poziționăm de cealaltă parte a baricadei şi preferăm să îl folosim atunci când încercăm să explicăm modul de funcționare a rețelelor. Nu facem altceva decât să fim de acord Cu Andrew Tanembaum: modelul

OSI a fost dezvoltat înaintea de a fi concepute protocoalele în timp ce modelul TCP/IP a apărut după ce au fost descrise protocoalele!

4.3 Infrastructura rețelei

Clienți, servere, imprimante, baze de date relaționale, toate acestea formează componentele unei rețele locale. Acestea sunt echipamente ce realizează încapsularea şi de-capsularea datelor pentru a-şi îndeplini toate sarcinile (transmitere mail-uri, editare texte, scanare, acces la baze de date). Continuăm prezentarea tehnologiilor prin prisma modelului OSI, începând cu nivelul fizic.

4.3.1 Cartela de rețea

Ce relație există între o placă de rețea (**N**etwork **I**nterface **C**ard) şi un computer? NIC este o placă cu circuite ce permite comunicarea în rețea: de la şi către un computer. Denumită şi *adaptor LAN*, *cartelă de rețea, placă de rețea, interfață de rețea* ea se montează într-un slot de extensie al plăcii de bază (PCI[21] de obicei) sau este chiar inclusă pe placa de bază, având un port prin care se realizează conectarea fizică în rețea a computerului.

Similar altor dispozitive hardware, cartela de rețea are nevoie de un *driver* (sau mai simplu un software) prin care să poată fi controlată. În cazul în care cartela este plug&play resursele sunt configurate în mod automat simplificându-se instalarea. În general, orice cartelă de rețea îndeplineşte următoarele funcții:

- pregătește datele pentru a putea fi transmise printr-un mediu;
- transmite datele;
- controlează fluxul datelor de la PC la mediul de transmisie.

Prin rețea datele circulă în serie (un bit odată, sau în serie) în timp ce în interiorul calculatorului circulă în paralel (16, 32 sau 64 biți odată, în funcție de bus-ul sistemului). Prin urmare, cartela de rețea trebuie să convertească datele care circulă în interiorul PC-ului în format serial.

Pentru a funcționa, fiecare NIC necesită o întrerupere (IRQ-Interrupt Request Line), o adresă I/O şi o adresă de memorie. Întreruperea o puteți asocia unei resurse prin care procesorul şi celelalte componente ale PC-ului îşi acordă atenție unele altora. Unele din aceste întreruperi sunt atribuite anumitor dispozitive chiar dacă acestea nu au fost încă instalate fizic în calculator (de exemplu LPT2 pentru o a doua imprimantă).

În cazul plăcilor de rețea, atribuirea unei întreruperi depinde de numărul întreruperii disponibilă pe calculator şi de numărul întreruperii prin care placa de rețea a fost proiectată să acceseze sistemul. Dacă întreruperea pe care este proiectată să lucreze placa de rețea este ocupată de alt dispozitiv, trebuie să rezolvați conflictul care apare reconfigurând cartela să lucreze pe altă întrerupere. Detalii despre toate întreruperile unui PC găsiți la adresa http://www.pcguide.com/ref/mbsys/res/irq**.**

Adresa de memorie (Memory I/O Address) va conține informații despre zona de memorie pe care respectivul dispozitiv şi sistemul de operare o vor folosi pentru a-şi transmite date. Intervalul uzual de adrese

[21] Standardul **Peripheral Component Interconnect** (**PCI**) defineşte specificațiile prin care perifericele unui calculator vor fi ataşate plăcii de bază

pe care o placa de rețea îl foloseşte este 0x240-0x360. O parte din aceste adrese sunt deja atribuite unor dispozitive. De exemplu adresa 0x278 este folosită de cel de al doilea port paralel iar 0x378 de primul. Cartele de sunet pot folosi 0x220 iar drive-urile CDROM pot folosi 0x300.

Pe lângă cartela de rețea clasică, ce necesită un cablu pentru a putea comunica, astăzi putem discuta şi de *cartelele wireless*[22].

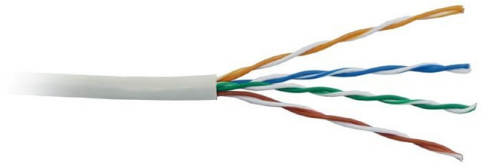
Spre deosebire de cartelele clasice, WNIC comunică prin intermediul unei antene. Pot fi instalate pe un slot PCI/PCMCIA[23], un port USB[24] sau pot fi integrate.

O cartele de rețea wireless poate opera în două moduri: *ad hoc* şi *infrastructură.* În primul caz, calculatorul poate comunica direct cu alte dispozitive fără a fi nevoie de alte echipamente sau configurații suplimentare. Singura condiție ce trebuie îndeplinită este ca toate dispozitivele în cauză să folosească acelaşi canal de comunicație.

În cel de al doilea caz avem nevoie de un *access point* (punct de acces). Calculatoarele care se conectează la acest access point trebuie să folosească acelaşi identificator al setului de servicii (SSID[25]). În cazul în care securitatea rețelei este asigurată cu ajutorul *Wired Equivalent Privacy (WEP)*[26] la nivelul access point-ului, toate calculatoarele trebuie să folosească aceeaşi cheie WEP.

4.3.2 Medii de transmisie „clasice"

Dacă PC-ul este dotat cu o NIC nu înseamnă că avem musai şi o rețea. Ca şi în cazul telefonului, mai este nevoie de un element prin care PC-ul nostru să poată fi legat la rețea. În această categorie intră mediile de transmisie sau cablurile, în limbaj rețelistic.



Unshielded Twisted-Pair (UTP)

Acest mediu de transmisie este format din patru perechi de fire, izolate între ele. Prin torsadarea perechilor de fire apare efectul de anulare, efect ce limitează degradarea semnalelor datorită interferențelor magnetice sau radio.

UTP-ul este un cablu uşor de instalat (are un diametru de aproximativ 0,4 cm) şi mult mai ieftin decât alte tipuri de cabluri. Deşi este considerat cel mai rapid mediu de transmisie bazat pe cupru, este mai vulnerabil în fața zgomotelor electrice în comparație cu alte categorii de cabluri.

Cablurile UTP din categoria 3 sunt formate din două fire izolate împletite împreună. O variantă mai performantă de astfel de cabluri este categoria 5. Acestea sunt similare celor din categoria 3 dar au mai multe răsuciri pe centimetru şi ar trebui să fie izolate cu teflon, rezultând de aici o interferență redusă şi o mai bună calitate a semnalului pe distanțe mari.

Conectorul standard folosit în cazul acestui cablu este RJ-45 (*Registered Jack*), asemănător cu cel de la firul telefonic. Conectorul este construit în baza unui standard din industria telefonică, standard care precizează care fir trebuie să fie conectat pe un anumit pin al

[22] Wireless Network Interface Card (WNIC)
[23] Personal Computer Memory Card International Association – specificațiile pentru cardurile ataşate laptop-urilor
[24] Universal Serial Bus (USB) – un port serial prin intermediul căruia pot fi ataşate mai multe dispozitive unui calculator
[25] SSID – o secvență de cod ataşată pachetelor transmise prin rețeaua wireless pentru a identifica pachetele ca făcând parte din acea rețea.
[26] Este cea mai simplă metodă de protecție a rețelelor wireless şi relativ simplu de depăşit.

conectorului.

Foiled twisted pair (FTP)

Cablul FTP se aseamănă cu UTP cu deosebirea că cele 4 perechi de fire sunt protejate de o folie de aluminiu. Deşi a fost proiectat pentru a fi folosit în zonele cu ecranare mare, la noi se foloseşte mai ales în rețele de cartier la cablarea între clădiri. Dezavantajul acestui cablu este dat tocmai de folia de aluminiu care trebuie să facă parte din circuit, asigurând împământarea.

Fibra optică

Fibra optică este mediul care asigură transmiterea luminii, modulată la o anumită frecvență. Comparativ cu alte medii de transmisie, fibra optică este cea mai costisitoare, dar nu este susceptibilă la interferențe electromagnetice şi în plus asigură rate de transfer mult mai ridicate decât celelalte categorii de medii.

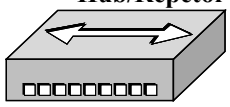
Cablul fibră optică constă în două fibre de sticlă îmbrăcate separat într-un înveliş de plastic (materialul se numeşte Kevlar). Cele două fibre formează inima acestui mediu de transmisie, sticla din care sunt realizate având un grad ridicat de refracție. Vom reveni cu mai multe detalii.

Prin prisma standardelor IEEE 802.3, Ethernetul foloseşte doar câteva din standardele existente în materie de cabluri: 10Base5, 10Base2, 10BaseT, 10 BaseF, 100BaseF. Notația anterioară înseamnă că rețeaua foloseşte o anumită lățime de bandă, utilizează semnalizarea în bandă de bază şi poate suporta segmente de diferite lungimi pe diferite medii de transmisie. Vom face o prezentare sintetizată a acestor standarde.

4.4 Echipamente de transmisie a datelor

Chiar dacă acest capitol tratează subiecte legate de nivelul 1 OSI, vom extinde puțin discuția prezentînd şi echipamentele care corespund nivelurilor 2 şi 3

Hub/Repetor



Termenul de repetor vine tocmai de la începuturile comunicării vizuale când, o persoană aflată pe un deal, repeta semnalul pe care tocmai îl primise de la o persoană aflată pe un alt deal situat în vecinătatea sa, pentru a-l transmite mai departe. Telegrafia, telefonia (mai ales cea mobilă) folosesc repetoare de semnal pentru a asigura transmiterea informațiilor la distanțe foarte mari.

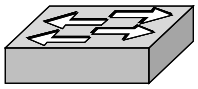
În limbajul cotidian, hub-urile din domeniul rețelelor mai sunt denumite şi repetoare (deşi nu prea este corect). Acestea pot fi *single port in – single port aut* (folosite în special pentru a depăşi limita impusă de lungimea maximă a unui segment), *stackable* (modulare) sau *multi port* (aceste sunt cunoscute mai ales sub denumirea de *hub*-uri). Ele sunt clasificate ca fiind componente de nivel 1 deoarece acționează doar la nivel de biți. **Nu uitați!** Scopul unui hub este de a amplifica şi a retransmite semnale, la nivel de bit, către un număr mai mare de utilizatori: 8,16, sau 24. Procesul prin care se realizează această funcție se numeşte concentrare.

Fiecare hub are propriul său port prin care se conectează la rețea şi mai multe porturi disponibile pentru calculatoare. Unele hub-uri au un port prin care pot fi legate de o consolă, ceea ce înseamnă că sunt hub-uri gestionabile/cu management. Majoritatea însă, sunt *dumb hubs* (hub-uri proaste) deoarece doar preiau un semnal din rețea şi îl repetă către fiecare port în parte.

Huburile se comportă ca şi cum ar fi mai multe calculatoare pe un cablu partajat, altfel spus un singur port transmite la un moment dat. Celelalte porturi şi implicit calculatoarele de la capătul legăturii răspund de detectarea eventualelor coliziuni şi de reluarea transmisiei în cazul apariției lor.

Principala problemă care apare în cazul folosirii hub-urilor o reprezintă coliziunea pachetelor pe segmentul respectiv de rețea.

Switch-ul/Comutatorul

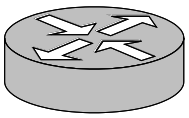


La prima vedere un switch seamănă foarte bine cu un hub, dar după cum vedeți, simbolul său arată un flux informațional bidirecțional.

Menirea acestui dispozitiv este de a concentra conectivitatea garantând în acelaşi timp lățimea de bandă. Switch-ul este un dispozitiv ce combină conectivitatea unui hub cu posibilitatea regularizării traficului pentru fiecare port. Ca manieră de lucru, el comută pachetele de pe porturile transmițătoare către cele destinatare, asigurând fiecărui port lățimea de bandă maximă a rețelei.

Această comutare a pachetelor se face pe baza adresei MAC, ceea ce face din switch un dispozitiv de nivel 2.

Router-ul[27]



Simbolul router-ului descrie foarte bine cele două funcții ale sale: selecția căii de transmitere a informațiilor şi comutarea pachetelor către cea mai bună rută.

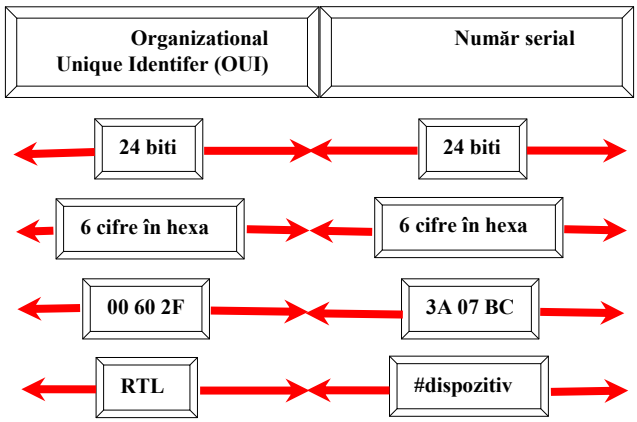
Fizic, routerele se prezintă sub o mulțime de forme, în funcție de model şi de producător. Componentele principale ale routerului sunt interfețele prin care rețeaua proprietară se conectează la alte segmente de rețea. Din acest motiv el este considerat un dispozitiv inter-rețele.

Scopul routerului este să examineze pachetele recepționate, să aleagă cea mai bună cale de transmitere a acestora şi în final să le transfere către portul corespunzător. Pentru rețelele mari, el reprezintă cel mai important dispozitiv prin care se reglează traficul rețelei. Deciziile routerului în ceea ce priveşte selectarea căii de rutare se iau pe baza informațiilor de la nivelul 3 (adresele de rețea), motiv pentru care sunt considerate echipamente de nivel 3. De asemenea, ele asigură conectivitate pentru diferitele tehnologii ale nivelului2: Ethernet, Token Ring, FDDI.

În concluzie:

Echipament	**Nivelul OSI la care lucrează**	**Protocol**	**Domeniu**	**Cu ce lucrează**
Repetoare/huburi	1	Transparent	Amplifică semnalul	Biti
Bridge	2	Transparent	Domeniu de coliziune	Cadre
Switch	2	Transparent	Domeniu de coliziune	Cadre
Ruter	3	Dedicat	Domeniu de broadcast	Pachete

27 În unele lucrări de la noi este denumit şi repartitor



Cum ziceam şi în introducere, teoria merge de mână cu practica. De aici şi încercarea noastră de a prezenta un posibil scenariu de depanare a problemelor care pot să apară la nivelul fizic al reţelei. Deşi suntem abia la nivelul 1 al modelului OSI este posibil să facem trimitere la lucruri nespuse încă. În acest caz trebuie doar să faceţi un salt înainte către paginile cu pricina.

4.5 Adresa MAC

The Institute of Electrical and Electronic Engineers (IEEE)[28] este organizaţia profesională care a definit standardele aplicabile în domeniul reţelelor de calculatoare:

- 802.1- modul de interconectare în reţea;
- 802.2- controlul legăturii logice (LLC);
- 802.3- reţele LAN cu acces multiplu şi cu detectarea purtătoarei şi a coliziunilor CSMA / CD, sau **reţelele Ethernet**[29];
- 802.4- reţele LAN cu transfer de jeton pe magistrală (Token Bus);
- 802.5- reţele LAN cu transfer de jeton în inel (Token Ring);
- 802.6- reţele metropolitane (MAN);
- 802.11- reţele fără fir pe baza CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance);
- 802.12-reţele LAN cu prioritate la cerere.

Când se vorbeşte de nivelul 2 se au în vedere şi cele două noi componente apărute în timp: LLC şi MAC:

- **Media Access Control** (MAC) – realizează tranziţia în jos, către mediul fizic de transmisie
- **Logical Link Control** (LLC)[30] - realizează tranziţia în sus, către nivelul reţea.

Subnivelul LLC este independent de tehnologia folosită, în timp ce MAC este dependent de tehnologia folosită.

Subnivelul MAC se ocupă de protocoalele pe care un calculator le foloseşte pentru a accesa mediul fizic de transmisie a datelor. Adresa MAC are o lungime de 48 de biţi, şi este exprimată în hexazecimal (12 cifre). Primele 6 care formează OUI (Organizational Unique Identifer), sunt administrate de către IEEE, identificând producătorul sau vînzătorul produsului. Celelalte 6, descriu numărul interfeţei (Serial Number Interface) sau o altă valoare administrată de fiecare producător sau vânzător.

Adresa MAC este „scrisă" în memoria ROM a cartelei de reţea, de unde este apoi copiată în RAM la iniţializarea cartelei. Prin urmare, dacă o cartelă este înlocuită, se va schimba şi adresa fizică a calculatorului.

Când un dispozitiv din cadrul unei reţele Ethernet încearcă să transmită date către alt dispozitiv, va căuta să deschidă un canal de comunicaţie cu acesta, folosind adresa MAC: datele transmise vor transporta şi adresa MAC a destinaţiei. Pe măsură ce datele traversează mediul fizic

---

[28] http://standards.ieee.org
[29] Pe larg la adresa http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm
[30] Definit prin IEEE 802.2

de transmisie, NIC-ul fiecărui calculator din rețea verifică dacă adresa sa MAC corespunde adresei destinație inclusă în pachet. Dacă adresele nu sunt identice, NIC ignoră datele din pachet, date ce continuă să circule către următoarea destinație. Dacă adresele sunt identice, NIC face o copie a pachetului cu date şi plasează această copie în calculator, la nivelul legătură de date. Pachetul original va continua să circule prin rețea, către alte destinații, unde se va verifica corespondența dintre adresele MAC.

Dezavantajul major al adresării MAC constă în faptul că aceste adrese nu au o structură strict definită: vânzătorii au OUI-uri diferite. Altfel spus, adresarea MAC nu este o adresare ierarhică, după cum se va vedea că este adresarea IP. Pe măsură ce rețeaua "creşte", acest dezavantaj devine o problemă majoră. Nu uitați: de fiecare dată când se discută de adresa MAC trebuie să vă gândiți la nivelul legătură date.

4.6 Adrese IP

Nivelul rețea joacă un rol important în transmisia datelor: foloseşte o schemă de adresare pe care se bazează echipamentele pentru a determina care este destinația datelor pe care le transmit.

Protocoalele care nu sunt suportate de nivelul 3 pot fi folosite doar în rețelele de dimensiuni mici. Aceste protocoale folosesc de obicei un nume pentru a identifica un calculator din rețea (cum ar fi adresa MAC). Dar, pe măsură ce rețeaua se dezvoltă, organizarea acestor nume devine un calvar. Dacă vrem să interconectăm între ele două subrețele va trebui să verificăm dacă numele calculatoarelor din cele două subrețele nu sunt duplicate.

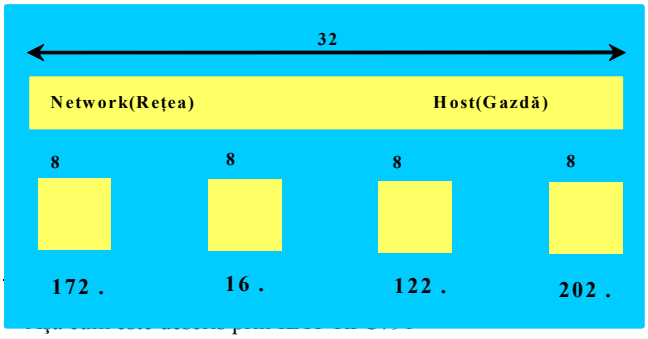
Internetul a ajuns astăzi o colecție de segmente de rețea care partajează în comun resurse informaționale. Echipamentele de nivel 3 folosite la interconectarea rețelelor sunt router-ele. Acestea sunt capabile să ia decizii logice cu privire la traseul cel mai bun pe care trebuie să-l urmeze un pachet prin rețea.

Internet Protocol reprezintă cea mai folosită schemă de adresare ierarhică la nivelul 3. Dacă aruncăm o privire asupra modelului OSI, vom observa că pe măsură ce informațiile străbat în jos nivelurile acestui model, datele sunt încapsulate la fiecare nivel. La nivelul rețea datele sunt transformate în datagrame, şi dacă rețeaua foloseşte adresarea IP, datele sunt transformate în datagrame IP.

În cazul telefoanelor mobile identificatorul unic al dispozitivului se numeşte IMEI - International Mobile Equipment Identity. Este un cod format din 14 caractere şi identifică originea, modelul şi un număr de serie al dispozitivului.

4.7 Protocolul IP versiunea 4 (IPv4)[31]

Elementul central al Internetului este protocolul de nivel rețea numit **IP (Internet Protocol).** Sarcina acestui protocol este de a oferi o cale pentru a transporta datagramele de la sursă la destinație, fără a ține seama dacă mașinile sunt sau nu în aceeași rețea sau dacă sunt sau nu alte rețele între ele.



O adresă IP conține informațiile necesare pentru a transporta un pachet cu date prin rețea şi este reprezentată printr-un

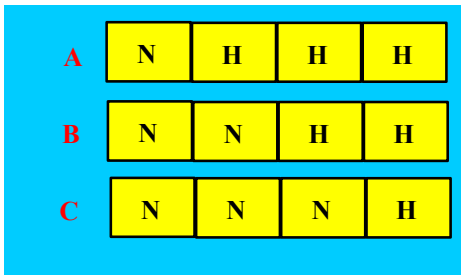
număr binar cu o valoare egală cu 32 biți.

Pentru a putea fi ușor de citit, adresa IP a fost împărțită în patru octeți, fiecare octet conținînd 8 biti. Valoarea maximă a fiecărui octet (în zecimal) este 255.

Orice adresă IP este logic împărțită în două zone. Prima zonă se numeşte *network id* şi identifică rețeaua căreia aparține un echipament. Cea de a doua zonă se numeşte *host id* şi identifică în mod unic dispozitivul conectat la rețea. Deoarece o adresă IP este alcătuită din patru octeți separați prin punct, primul, al doilea sau al treilea dintre aceştia pot fi folosiți pentru a identifica rețeaua din care face parte un dispozitiv. La fel şi pentru identificarea dispozitivului în sine.

Există trei clase de adrese IP comerciale, clase gestionate de InterNIC: clasa A, B şi C (mai există D şi E dar acestea nu sunt comerciale). Clasa A este rezervată de InterNIC organizațiilor guvernamentale (mai mult guvernelor) din lumea întreagă; clasa B este rezervată organizațiilor medii-mari, iar clasa C este rezervată oricărui alt tip de organizație.

Când o adresă din clasa A este scrisă în format binar, primul bit este întotdeauna *0*. Primii doi biți ai unei adrese din clasa B sunt *10*, iar primii trei biți ai unei adrese din clasa C sunt întotdeauna *110*. Un exemplu de adresă IP din clasa A: 124.95.44.15. Primul octet (124) identifică numărul rețelei atribuit de InterNIC. Administratorul acestei rețele va atribui valori pentru restul de 24 biți. O manieră ușoară prin care puteți să recunoaşteți dacă un dispozitiv face parte dintr-o rețea de clasă A, presupune să analizați primul octet al adresei IP. Numerele din primul octet al adreselor din clasa A sunt cuprinse între **0 şi 127**.



Toate adresele IP din clasa A folosesc doar primii 8 biți pentru a identifica porțiunea „network" din cadrul unei adrese. Restul de trei octeți din cadrul adresei sunt rezervați porțiunii „host" din cadrul acesteia. Cea mai mică adresă ce poate fi atribuită unui host va avea toți biții din cadrul ultimilor trei octeți la valoarea 0. Cel mai mare număr ce poate fi atribuit porțiunii host va avea toți biții din ultimii trei octeți la valoarea 1.

Orice rețea care face parte dintr-o clasă A de adrese IP poate să conțină teoretic 2^{24} host-uri (adică 16.777.214).

Un exemplu de adresă din clasa B: 151.10.13.28. Primii doi octeți identifică numărul rețelei atribuit de InterNIC. Administratorul unei astfel de rețele poate să atribuie valori următorilor 16 biți. Când vreți să recunoaşteți dacă o adresă este din clasa B analizați primii doi octeți ai adresei. Aceste adrese au întotdeauna valori cuprinse între **128-191** pentru primul octet şi între **0-255** pentru cel de al doilea octet.

Toate adresele din clasa B folosesc primii 16 biți pentru a identifica porțiunea "network" din cadrul unei adrese. Ultimii 2 octeți sunt rezervați porțiunii "host". Orice rețea care foloseşte adrese din clasa B poate atribui teoretic 2^{16}(65.534) adrese IP echipamentelor care sunt ataşate acesteia.

O adresă din clasa C: 201.110.213.28. Primii trei octeți identifică numărul rețelei atribuit de către InterNIC. Administratorul de rețea poate atribui valori doar ultimului octet. Cum puteți recunoaşte o adresă din clasa C? Analizați primii trei octeti: primul octet ia valori între **192-223**, al doilea şi al treilea octet pot să ia valori între **1-255**. Toate adresele din clasa C folosesc primi 24 biți pentru a identifica rețeaua din care face parte un dispozitiv. Doar ultimul octet este rezervat porțiunii "host" Orice rețea care foloseşte adrese din clasa C poate aloca teoretic 2^8(256) adrese echipamentelor ataşate acesteia.

Orice adresă IP identifică un echipament într-o rețea şi rețeaua căruia aparține. Dacă, spre exemplu, calculatorul vostru vrea să comunice cu altul din rețea, ar trebui să ştiți adresa IP al celui din urmă. De fapt ar trebui să ştiți adresele tuturor calculatoarelor cu care vreți să comunicați. Ar fi complicat, nu? Din fericire acest neajuns este rezolvat de alții.

Adresele IP care au toată porțiunea de host cu valoarea 0 sunt rezervate ca adrese de rețea. De exemplu o adresă din clasa A 113.0.0.0 reprezintă adresa IP pentru rețeaua 113. Un ruter va folosi această adresă pentru a transmite datele în Internet.

Să luăm ca exemplu o adresă din clasa B. Primii doi octeți nu pot fi zero pentru că valorile lor sunt atribuite de InterNIC şi reprezintă numerele rețelelor respective. Doar ultimii doi octeți pot fi 0, deoarece numerele din aceşti octeți reprezintă numărul host-urilor şi sunt rezervate dispozitivelor atașate respectivei rețele. Pentru a putea comunica cu toate dispozitivele din rețea, adresa IP trebuie să conțină 0 în ultimii doi octeți. O astfel de adresă ar fi de exemplu 176.10.0.0.

Când se transmit date către toate echipamentele dintr-o rețea trebuie creată o adresă de broadcast (difuzare). Broadcast-ul apare când stația sursă transmite date către toate celelalte dispozitive din rețeaua respectivă. Dar pentru a fi sigură că toate aceste dispozitive sunt "atente" la mesajul broadcast, stația sursă trebuie să folosească o adresă IP pe care să o recunoască toate celelalte echipamente din rețea. De obicei, într-o astfel de adresă, bitii din porțiunea host au toți *valoarea 1*. Pentru rețeaua folosită în exemplul anterior, adresa de broadcast va fi 176.10.255.255. (Vezi şi *http://www.ralphb.net/IPSubnet*)

Într-o rețea, hosturile pot comunica între ele doar dacă au acelaşi identificator de rețea (porțiunea *network id* este identică). Acestea pot să partajeze acelaşi segment fizic de rețea, dar dacă au identificatori de rețea diferiți, nu pot comunica decât dacă există un alt dispozitiv care să realizeze conexiunea între segmentele logice ale rețelei (sau identificatorii acestora). (Puteți asemui aceşti identificatori de rețea cu codul poştal).

După cum am arătat deja, fiecare clasă de adrese IP permite un număr fix de hosturi. Dar nu trebuie să uitați că *prima* adresă din fiecare rețea este rezervată pentru a *identifica rețeaua*, iar ultima *adresă* este rezervată pentru *broadcast*

4.8 Protocolul IP versiunea 6 (IPv6)

Am menționat la un moment dat că CIDR a fost soluția de compromis până la dezvoltarea versiunii 6 a protocolului IP[32]. Chiar dacă tehnologiile Internetului sunt dominate încă de versiunea 4 se consideră că până la sfârşitul anului 2025 bugurile şi erorile care vor fi descoperite la nivelul acestei noi versiuni vor fi rezolvate si standardizarea va fi deplin[

Principala modificare pe care o aduce IPv6 ține de lungimea adresei: 128 biți exprimați în format hexazecimal, ceea ce înseamnă 2^{128} adrese (sau 340.282.366.920.938.463.463.374.607.431.768.211.456 adrese!). Nu este scopul nostru să intrăm în detalii legate de acest subiect ci doar să vă anunțăm că tehnologia se modifică de la o zi la alta şi la noi.

Tehnicismele specifice protocolului sunt puțin diferite la această versiune față de cea anterioară. Noi vă prezentăm câteva din argumentele (mai multe detalii în RFC-urile menționate) care vor face din IPng protocolul nivelului rețea folosit nu doar pentru extinderea spațiului de adresare:

- *Capacități extinse de adresare – capacitați extinse de rutare*
- *Apariția adreselor de tip "anycast"*
- *Formatul antetului (headerului) simplificat față de IPv4*
- *Facilități pentru asigurarea calității serviciilor (QoS)*
- *Facilități de autentificare şi asigurarea confidențialității prin criptare*

[32] Definit prin RFC: 1924, 2374, 2460, 2463, 2464, 3513

Capitolul 5. Scena producerii infracțiunii informatice

Locul în care se realizează o infracțiune cu ajutorul calculatorului necesită o cunoaştere extinsă a prelucrărilor electronice, a tehnologiei şi modului de colectare a datelor. Securizarea locului este parte integrantă a procesului investigativ.

5.1. Securizarea şi evaluarea scenei

După securizarea fizică a locului unde s-a produs o infracțiune, investigatorul trebuie să identifice vizual toate probele potențiale şi să se asigure că integritatea fizică şi logică a acestora nu va fi afectată.

Probele digitale pot fi foarte uşor şterse, distruse sau alterate.
Dacă un dispozitiv nu este alimentat cu energie electrică trebuie lăsat în această stare. În situația în care la prima vedere nu se poate determina starea dispozitivului se vor vizualiza led-urile indicatoare sau se ascultă dacă este pornit (în cazul sistemelor de calcul, ventilatoarele produc un zgomot ce poate fi auzit cu uşurință).
Chiar dacă partea documentară o abordăm separat în următorul subcapitol, menționăm că încă din acest moment este bine să produce propriile dovezi care vor asigura trasabilitatea investigației.

Fişă de evaluare preliminară pentru dispozitivul: _____	
Numele utilizatorilor	
Numele de login/contului de acces	
Parole identificate şi aplicații corespondente	
Aplicații în uz	
Tipul conexiunii Internet	
Dispozitive de stocare externe	
Documentații ale aplicațiilor instalate	
Conturi de e-mail şi clienți de e-mail	
Aplicații de securitate în uz	
Restricții privind accesul la date/resurse locale	
Aplicații/facilități de criptare	
Dispozitive/aplicații destructive	
Conturi de acces la rețele	

de socializare (Facebook, Twitter)	
Alte Informații	

Pornind de la un prim element identificat la locul infracțiunii, căutarea altor probe se poate face în spirală, în linie sau tip grilă.

Dacă pe monitor se poate identifica o aplicație activă, o imagine, email sau un site Internet sau dacă monitorul este pornit dar nu se afișează nimic primul lucru ce trebuie întreprins este fotografierea display-ului/monitorului. Apoi se mișcă puțin mouse-ul pentru a identifica dacă nu este activ screen-saverul.
Tot ce se identifică se documentează.
Dacă monitorul nu este pornit dar calculatorul este alimentat cu energie electrică, se pornește monitorul din buton și se fotografiază ceea ce afișează.

Foarte important! Înainte de consultarea probelor în formatul lor electronic, prin accesarea dispozitivelor de calcul sau de stocare, incluzând calculatoare, servere, laptop, tablete, telefoane mobile, dispozitive GPS, investigatorul trebuie să obțină un mandat de percheziție informatică, conform Legii 161/2003[33] TITLUL III Prevenirea și combaterea criminalității informatice
Mandatul de percheziție informatica se poate obține si ulterior de la un judecător - in cazul in care investigatorul nu avea decât un mandat de percheziție domiciliar și percheziția informatică se justifică prin asimilare cu cazul inițial.

5.2. Documentarea scenei

Ca auditor (CISA) am învățat că orice concluzie se bazează pe dovezi. Iar dovezile trebuie să fie suficiente, corespunzătoare și de încredere[34]. Aceste cerințe se aplică și în cazul investigațiilor informatice pentru că scopul este același: asigurarea trasabilității investigației.

Trebuie să ținem cont de faptul că documentarea inițială poate implica schimbarea poziției unor dispozitive. Pornind de la acest fapt documentarea ar trebui să includă o înregistrare video detaliată sau fotografierea locului cu scopul de a recrea detaliile locului în orice moment ulterior.

Așa cum am menționat anterior, tot ceea ce se identifică pe monitoarele găsite pornite trebuie documentat în foi de lucru (nu există o standardizare în acest sens). Nu trebuie uitat că în domeniul tehnologiilor informaționale avem de a face cu multe aspecte intangibile și de la un anumit loc de unde pot fi identificate probe se poate ajunge și la alte locuri aflate în alte zone geografice.

Circumstanțele de la locul infracțiunii pot să conducă la situații în care nu este posibilă colectarea tuturor probelor de la locul infracțiunii.

Despre documentare vom mai face vorbire cu referire însă la probe.

5.3. Colectarea probelor

Riscul cel mai mare cu care se poate confrunta un investigator îl reprezintă alterarea integrității dispozitivului sau a datelor conținute de acesta. De exemplu, dacă pe un calculator este

[33] Legea 161 din 19/04/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției
[34] Vezi standardul ISACA S14 Audit Evidence, ghidul ISACA G2 Audit Evidence Requirement

activată criptarea şi este întreruptă alimentarea cu energie electrică, există o mare probabilitate ca datele să nu mai poată fi accesate ulterior. Toate activitățile şi acțiunile întreprinse asupra dispozitivelor electronice se realizează purtând mănuşi pentru a nu compromite sau distruge probele fizice. Cu excepția investigatorului sau a unui membru al echipei acestuia nici unei alte persoane nu trebuie să i se permită accesul la dispozitivele investigate.

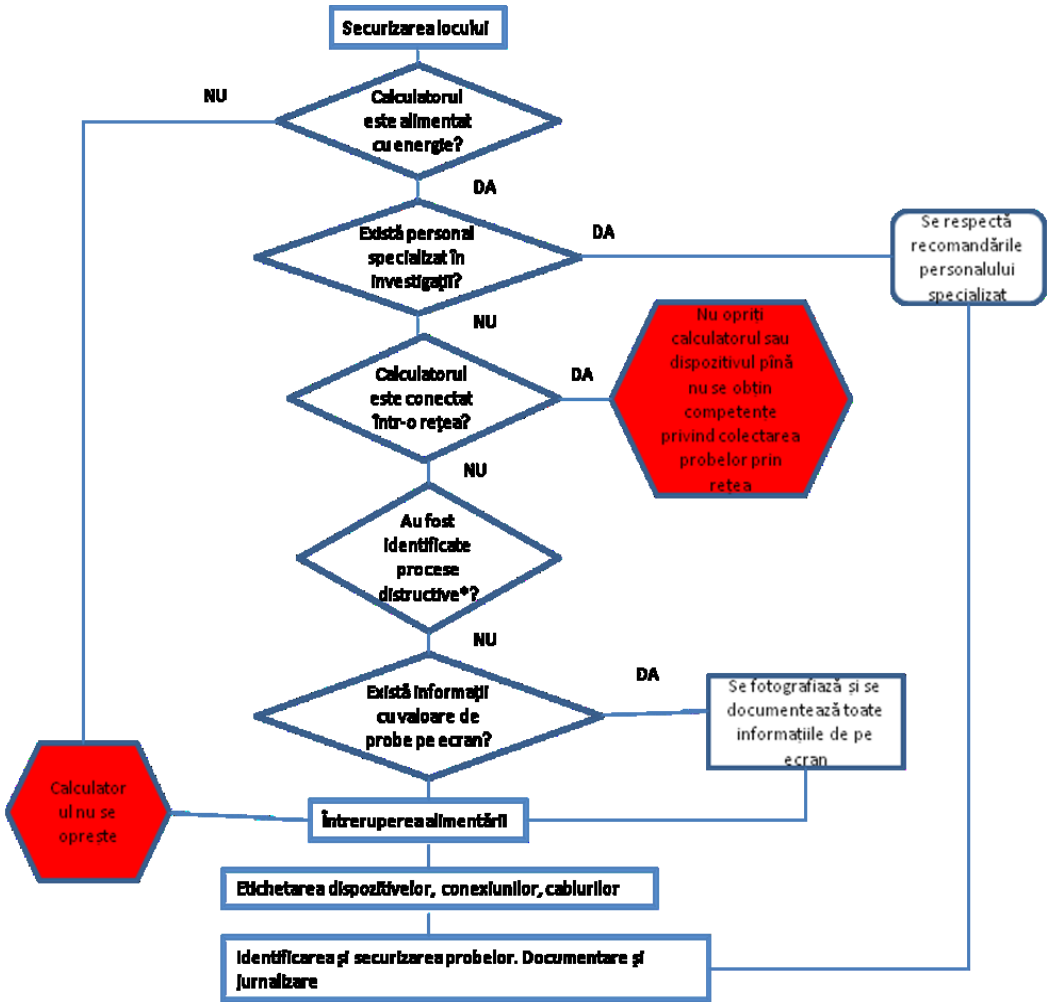

Securizarea locului
Calculatorul este alimentat cu energie?
NU
DA
Există personal specializat în investigații?
DA
Se respectă recomandările personalului specializat
NU
Calculatorul este conectat într-o rețea?
DA
Nu opriți calculatorul sau dispozitivul până nu se obțin competențe privind colectarea probelor prin rețea
NU
Au fost identificate procese distructive*?
NU
Există informații cu valoare de probe pe ecran?
DA
Se fotografiază și se documentează toate informațiile de pe ecran
Calculatorul nu se oprește
Întreruperea alimentării
Etichetarea dispozitivelor, conexiunilor, cablurilor
Identificarea și securizarea probelor. Documentare și jurnalizare

Figura nr. 5.1 – *Procedura de colectare a probelor informatice*

Pornind de la etapa a 2 a din schema de mai sus vom exemplifica 4 situații cu care investigatorul se poate întâlni în practică

Studiu de caz 1: Calculatorul este pornit iar monitorul afişează anumite informații

- Se fotografiază monitorul şi se documentează informațiile afişate pe acesta
- Dacă informațiile de pe ecran indică că datele vor şterse (delete, remove) sau rescrise (format) se deconectează dispozitivul de la sursa de alimentare
- Se va verifica dacă acesta nu are activată opțiunea de acces de la distanță.

- Dacă există o conexiune activă la Internet se verifică starea mesageriei electronice, a mesageriei instant şi a camerei web.
- Dacă datele afişate pe ecran au valoare de probă se trece la colectarea acestora

Studiu de caz 2: Calculatorul este pornit iar monitorul afişează screen saver-ul sau o imagine statică

- Se mişcă **doar** mouse-ul sau se atinge pad-ul (în cazul lap top-urilor). Apăsarea oricărei taste sau a butoanelor mouse-ului este interzisă.
- Se fotografiază şi se documentează informaţiile afişate pe ecran.

Studiu de caz 3: Calculatorul este pornit iar monitorul pare a fi oprit

- Se mişcă **doar** mouse-ul sau se atinge pad-ul (în cazul lap top-urilor).
- Dacă monitorul afişează informaţii se fotografiază şi documentează
- Dacă monitorul este oprit (nu s-a identificat nici un indicator care să certifice starea acestuia) se porneşte şi se fotografiază şi documentează informaţiile afişate.

Studiu de caz 4: Calculatorul este oprit

- Se fotografiază şi se documentează (inclusiv etichetare) toate cablurile şi dispozitivele ataşate.
- Se deconectează calculatorul de la priză şi toate cablurile şi dispozitivele ataşate
- Se sigilează sursele de alimentare, butoanele, porturile de conectare a altor dispozitive, drive-urile asociate (CD-ROM, flopy disk, dacă există).
- Se documentează modelul dispozitivului, numărul serial etc.
- Se împachetează conform procedurilor

Atenţia cuvenită trebuie acordată şi probelor non digitale existente la locul infracţiunii: documentaţii, notiţe, manuale de utilizare. Un posibil model de foaie de lucru este prezentat mai jos:

Informaţii despre calculator:

Producător:_____Model_____
Număr serial:_____
Desktop ☐ Laptop☐ Server☐ Altu☐
Stare bună ☐ Distrus/avariat ☐
Număr hard disk_____3.5 Floppy drive☐ Uitate bandă ☐ip drive_____
Modem ☐ Cartelă reţea ☐ DVI☐ Tip drive_____
USB☐ Număr porturi_____
Cititor carduri ☐ Tip carduri_____
Altele:_____

Informaţii CMOS☐
Parolă logon ☐ Parolă_____
Data şi ora curentă_____
Data şi ora CMOS_____

Setări hard drive CMOS
Auto ☐
Capacitate_____Nr. cilindri_____Nr. capete_____Nr. sectoare_____
Mod: LBA ☐ Normal☐ Auto ☐

Modelul de mai sus este doar un punct de pornire. Trebuie colectate cât mai multe informații astfel încât să nu se poată afirma ulterior că s-a intervenit fizic asupra calculatorului. O parte din informațiile documentate în foaia de lucru prezentată ca model pot fi detaliate şi documentate separat. De exemplu în cazul hard disk-urilor se vor documenta: etichetele asociate volumelor; numărul de partiții fizice şi logice; dacă sunt boot-abile sau nu; tipul controller-ului etc.

5.4. Ambalarea, transportul şi păstrarea probelor digitale

În cele mai multe cazuri se impune ca achiziția datelor să nu se facă în acelaşi loc în care a avut loc infracțiunea. Situațiile în care acest lucru nu este posibil sunt rare. În paragraful anterior am folosit foarte des cuvântul „documentare" pentru a evidenția că orice acțiune întreprinsă de investigator trebuie documentată şi înregistrată. Documentarea investigației poate fi la rândul său probă!

Înainte de a se trece la împachetarea probelor, investigatorul trebuie să verifice dacă au fost documentate toate activitățile ce au vizat identificarea, colectarea, etichetarea, fotografierea şi inventarierea. Probele biologice latente vor fi recoltate abia după colectarea şi analizarea probelor digitale.

Împachetarea trebuie să se facă cu materiale antistatice fiind permisă folosirea doar a hârtiei sau cutiilor de carton. Nu vor fi folosite materiale plastice la împachetare. Împachetarea trebuie să asigure protecție împotriva deformării sau zgârierii suprafețelor magnetice.

Nu am intrat până acum în detalii privind telefoanele mobile sau telefoanele inteligente. Acestea se lasă exact în starea în care au fost identificate şi se împachetează în materiale în materiale care izolează radio frecvențele (se acceptă şi folie de aluminiu). Izolate astfel aceste dispozitive se transportă la laboratorul unde se vor realiza investigațiile.

Pe parcursul transportului de la locul infracțiunii la laboratorul de investigații trebuie să se asigure şi să se documenteze lanțul de custodie. Probele se predau şi se recepționează pe bază de semnătură!

În ceea ce priveşte păstrarea probelor digitale este important să se asigure condițiile de mediu pe care producătorul echipamentului le-a impus, evitându-se umiditatea şi temperaturile extreme, expunerea la câmpuri magnetice etc.

Capitolul 6. Achiziția datelor

Procesul de investigare urmăreşte trei etape principale: achiziția datelor, analiza acestora şi raportarea. Achiziția datelor presupune copierea acestora de pe medii de stocare electronice, fără a fi alterate. În acest moment putem să avem în vedere două tipuri principale de date: date statice şi date volatile. Probabil în viitorul nu prea îndepărtat, concentrarea va fi asupra datelor volatile. Pentru a înțelege însă mai bine cum stau lucrurile ne vom îndrepta atenția asupra diferitelor tipuri de formate ale datelor cu mențiunea că există două modalități de achiziție a datelor: statică, respectiv dinamică.

6.1 Formate de stocare a datelor pentru probele digitale

Majoritatea aplicațiilor folosite în achiziționarea datelor în timpul investigațiilor folosesc formate proprietare (cu avantaje şi dezavantaje) precum şi formatul „raw". Acesta din urmă este un format open-source ce este înlocuit în ultimul timp de Advanced Forensic Format (AFF).

6.1.1. Formatul Raw

Până nu demult timp în urmă, singura variantă prin care se putea realiza copierea datelor în vedere examinării şi conservării acestora ca probe într-o investigație presupunea copierea lor bit cu bit de pe un suport magnetic/electronic pe altul. Prin această tehnică se realizau fişiere secvențiale dintr-un anumit set de date. Deoarece majoritatea aplicațiilor folosite în cadrul investigațiilor informatice pot citi astfel de fişiere, formatul „raw" este unul din formatele universale folosite în achiziția datelor chiar dacă necesită acelaşi spațiu de stocare ca fişierele originale analizate.

Majoritatea aplicațiilor comerciale realizează şi o validare a datelor achiziționate prin utilizarea Cyclic Redundancy Check (CRC-32), Message Digest 5 (MD5) sau Secure Hash Algorithm (SHA).

6.1.2. Formate proprietare furnizorilor de soluții informatice

Spre deosebire de formatul raw, formatele proprietare furnizorilor de soluții pentru investigații oferă în primul rând posibilitatea comprimării datelor achiziționate. Astfel se reduce necesarul de spațiu de stocare al probelor. Pe lângă această facilitate mai există posibilitatea segmentării unei imagini precum şi salvarea meta-datelor unui fişier supus analizei.

Principalul dezavantaj al formatelor proprietare constă în imposibilitatea partajării unei imagini între soluții diferite.

6.2. Metode de achiziție a datelor

Indiferent dacă avem în vedere achiziția statică sau dinamică, datele pot fi colectate prin patru metode:

- realizarea unui fişier imagine după un disc
- realizarea unei copii tip disc la disc

- realizarea unui disc logic după un disc fizic sau a unui fişier cu date după un disc
- realizarea unei copii după un fişier sau director şters.

Nu există o regulă general valabilă după care trebuie folosită una sau alta din metodele menționate. Acest lucru depinde în principal de situația din timpul şi de la locul investigației. Majoritatea aplicațiilor (FTK, EnCase, ProDiscover) folosesc metoda realizării unui fişier imagine după un disc, copii care este o replică bit cu bit a drive-ului original.

În situațiile în care această metodă nu poate fi aplicată (cazul drive-urilor de generații mai vechi) se foloseşte metoda disc la disc. Trebuie să spunem că această activitate este consumatoare de timp când discutăm de discuri de capacitate mare şi foarte mare (terabytes). Din acest motiv achiziția logică, altfel spus identificarea prealabilă a datelor ce prezintă interes pentru scopul investigației este metoda care ar trebui să fie aplicată.

Pentru a determina care din cele metode enumerate trebuie aplicată, ar trebui să avem în vedere dimensiunea discului considerat suspect, dacă discul poate fi reținut ca probă sau trebuie înapoiat proprietarului de drept, timpul disponibil pentru realizarea achiziției şi locul în care se află proba.

6.3. Protecţia la scriere

Ori de câte ori achiziționează date, investigatorul trebuie să se asigure că aceste nu vor fi alterate. Atunci când ataşam un dispozitiv de stocare a datelor la un calculator pe care rulează o versiune a sistemului de operare Windows, acesta poate scrie o semnătură pe acel dispozitiv, alertând prin aceasta conținutul. Pentru a preveni astfel de situații se recomandă blocarea la scriere a dispozitivelor (excepție fac cele proiectate astfel încât datele odată scrise nu mai pot fi alterate).

Acest lucru se realizează fie prin mecanismele proprietare ale dispozitivului hardware analizat fie cu ajutorul software-ului. Detalii despre acest subiect în capitolul următor.

Capitolul 7. Sistemul de fişiere şi regiştrii WINDOWS

Procesul de interpretare a probelor este unul laborios, care presupune utilizarea unor instrumente dedicate, sau în cazuri speciale apelarea directă la instrumentele sistemelor de operare. Secţiunile următoare descriu câteva aspecte tehnice ale organizării fişierelor şi reprezentării informaţiilor cu scopul de a înţelege, accesa şi interpreta mai uşor probele digitale.

7.1. Sistemul de fişiere

Cele mai importante sisteme de fişiere suportate de sistemele de operare Windows sunt: **FAT32 (File Allocation Table)** şi **NTFS (*New Technology File System*)[35].**

FAT 32

Acest sistem de fişiere a fost introdus de Microsoft pentru prima dată odată cu lansarea sistemului de operare Windows 95 OSR2. Spre deosebire de versiunile anterioare FAT 32 poate suporta (teoretic) discuri de până la 2TB datorită reducerii dimensiunii clusteri-lor şi prin urmare utilizarea mult mai eficientă a spaţiului de pe disk.

Dimensiunea clusteri-lor FAT32

Dimensiunea partiţiei	Dimensiunea cluster-ului
< 260 MB	**512 bytes**
260 MB - 8 GB	**4,096 bytes**
8 GB - 16 GB	**8,192 bytes**
16 GB - 32 GB	**16,384 bytes**
32 GB - 2 TB	**32,768 bytes**

În practică, pot fi formatate nativ FAT 32 doar partiţiile de până la 32GB. Dincolo de această dimensiune trebuie folosit FastFAT. Fără a mai insista asupra acestui subiect mai adăugăm doar că discurile formatate FAT 32 **nu oferă nativ nici un nivel de securitate, criptare sau comprimare a fişierelor.** Pentru o firmă acest lucru poate produce numeroase probleme în sistemul informaţional, motiv pentru care nu mai insistăm asupra acestui subiect.

NTFS 5

Sistemul de fişiere NTFS este soluţia cea mai folosită în cazul platformelor Windows. În continuare vom prezenta doar principalele facilităţi oferite de versiunea 5 a NTFS.

Cele mai multe hard discuri sunt divizate în mai multe secţiuni logice denumite *partiţii.* Pentru a analiza la nivel fizic o partiţie cu scopul de a afla informaţii despre antetul fişierelor (header) sau sistemul de operare utilizat putem folosi un editor de discuri (WinHex[36], Norton DiskEditor[37]).

---

[35] Pe larg despre acest subiect la adresa http://www.ntfs.com/

36 http://www.winhex.com/winhex/

37 http://us.norton.com/norton-utilities

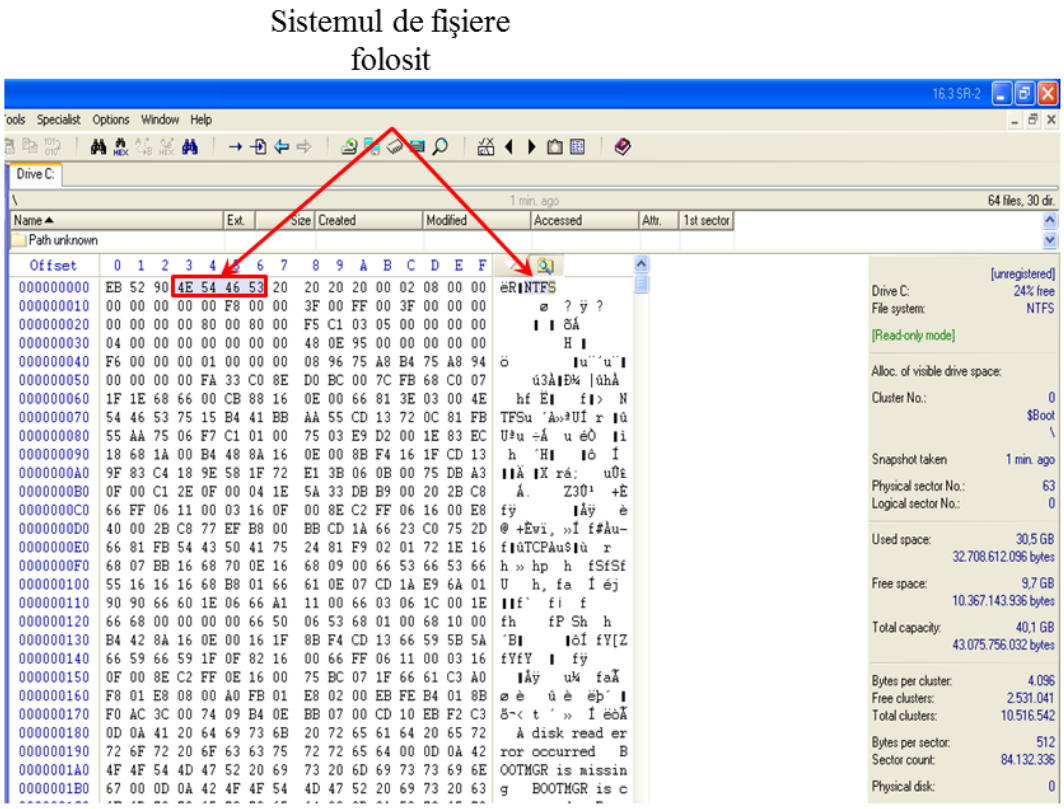


Figura nr. 7.1 – *Identificarea sistemului de fişiere folosit pe o unitate de stocare*

În figura de mai sus, în partea dreaptă apar şi informaţii despre *clustere*. Structura de fişiere folosită de Microsoft grupează sectoarele de pe un hard disk în clustere. Combinarea sectoarelor are drept scop scurtarea timpului necesar scrierii/citirii informaţiilor pe hard disk. Numărul de sectoare ce se combină pentru a forma un cluster depinde de dimensiunea hard diskului.

Numerotarea clusterelor se face secvenţial începând cu cifra 2 deoarece primul sector de pe fiecare hard disk conţine o zonă rezervată sistemului de operare, înregistrările necesare boot-ării şi baza de date cu structura fişierelor. Sistemul de operare este cel care alocă aceste cifre denumite adrese logice ai numărul sectorului reprezintă adresa fizică. Un cluster şi adresa sa sunt specifice unui disk logic (o partiţie a discului fizic).

Permisiuni la nivel de fişiere

Acesta este probabil cea mai utilizată facilitate a sistemului de fişiere. Pe un volum NTFS se pot preciza permisiuni la nivel de director şi/sau fişiere. Acest lucru înseamnă că se pot indica exact grupurile de utilizatori sau utilizatorii individuali cărora li se acordă permisiuni şi nivelul de acces permis.

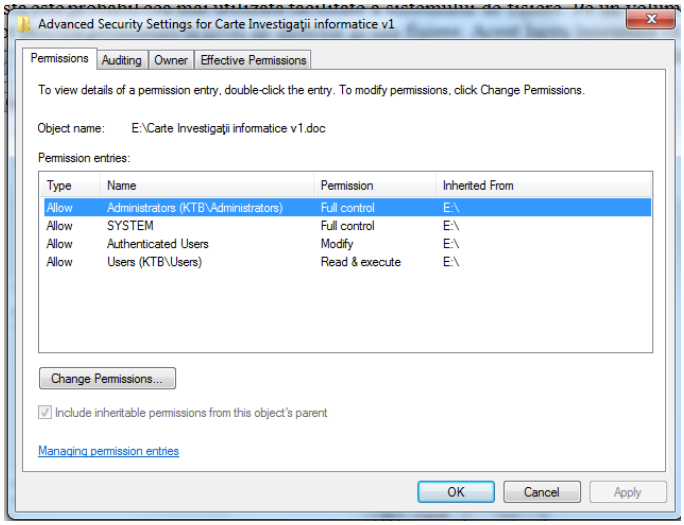


Figura nr. 7.2 – *Lista de control acces asupra fişierului de pe discul E*

Aceste permisiuni sunt gestiune prin intermediul *listelor pentru controlul discreţionar al accesului (DACL*[38]*)*.Permisiunile la nivelul unui volum NTFS vor fi moştenite implicit de toate obiectele respectivului volum.

Fiecare dosar şi fişier dintr-o partiţie NTFS are asociată câte o listă ACL (Access Control List – listă care controlează accesul). În lista ACL se află înscrise perechi de informaţii de tipul: ce utilizator (sau grupuri, sau eventual calculatoare) au acces şi ce tip de acces le este permis. Pentru ca un utilizator să aibă acces la un dosar sau fişier el trebuie sa fie cuprins în lista ACL (direct sau indirect, prin apartenenţa la un grup). Dacă utilizatorul nu apare în lista ACL atunci el nu are acces la acel obiect. În funcţie de tipul de utilizator, aceste drepturi de acces pot fi:

Drepturi restrânse: Full control (control deplin), Modify (modifică), Read&Execute (citeşte şi execută), List folder contents (listează conţinut folder), Read (citeşte), Write (scrie);

Drepturi extinse: Full control (control deplin), Traverse folder/execute file (traversează folder/execută fişier), List folder/read data (listează folder/citeşte date), Read attributes (citeşte atribute), Read extended attributes (citeşte atribute extinse), Create files/write data (creează fişiere/scrie date), Create folders/append data (creează foldere/adaugă date), Write attributes (scrie atribute), Write extended attributes (scrie atribute extinse), Delete subfolders and files (şterge subfoldere şi fişiere), Delete (şterge), Read permissions (citeşte permisiuni), Change permissions (schimbă permisiuni), Take ownership (ia în posesie).

Spre deosebire de versiunile anterioare ale SO, lucrul cu permisiunile se complică oarecum pentru că trebuie lucrat la nivel de *permisiuni efective* (ultimul tab din figura anterioară). Dacă nu se acordă atenţia cuvenită se poate întâmpla ca unui utilizator căruia i-aţi restricţionat accesul să poată totuşi efectua anumite schimbări.

Să luăm cazul prezentat în imaginea următoare. În directorul *Carte* în care am salvat fişierul *carte.doc* am acordat permisiuni de tip *full control* pe acest director, dar nu acord aceleaşi permisiuni şi pe fişierul amintit. Cu toate acestea, utilizatorii care vor avea acces la director vor putea să şteargă şi fişierul. De ce se întâmplă acest lucru? O fi vreun bug?

Permisiunile acordate pe directorul *Carte* includ şi *Delete Subfolders and Files*. Acestea sunt permisiuni speciale care apar în tab-ul aferent.

[38] Fiecare obiect creat de către sistemul de operare aparţine unui proprietar de drept. Doar proprietarul acelui obiect poate schimba permisiunile asociate acestuia, accesul fiind deci la *discreţia acestuia*

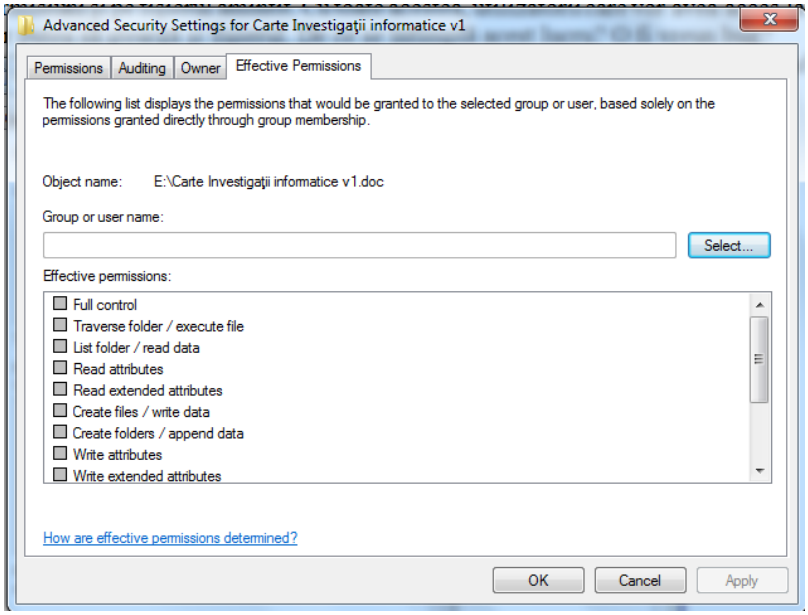

Advanced Security Settings for Carte Investigaţii informatice v1
Permissions
Auditing
Owner
Effective Permissions
The following list displays the permissions that would be granted to the selected group or user, based solely on the permissions granted directly through group membership.
Object name: E:\Carte Investigaţii informatice v1.doc
Group or user name:
Select...
Effective permissions:
Full control
Traverse folder / execute file
List folder / read data
Read attributes
Read extended attributes
Create files / write data
Create folders / append data
Write attributes
Write extended attributes
How are effective permissions determined?
OK
Cancel
Apply

Figura nr. 7.3 – *Permisiunile efective pe un fişier*

Pentru a evita situaţiile neplăcute precum cea prezentată anterior trebuie să verificaţi permisiunile efective atribuite obiectelor la care doriţi să restricţionaţi/controlaţi accesul, să nu lăsaţi activă opţiunea prin care se moştenesc permisiunile atribuite directorului (inherit) şi să resetaţi drepturile acordate anterior.

Criptare la nivel de fişier/director

NTFS-ul oferă şi facilităţi de criptare folosind o cheie simetrică pentru protecţia directoarelor şi fişierelor. Această facilitate este total transparentă pentru utilizatori autorizaţi: un fişier poate fi deschis, se poate lucra cu el iar la terminare are loc criptarea. Doar utilizatorii neautorizaţi vor fi avertizaţi prin clasicul "Access denied" că nu li se permite accesarea directoarelor/fişierelor. Pentru a fi siguri de setările pe care le faceţi, activaţi criptarea la nivel de director. Astfel toate fişierele din respectivul director vor fi automat criptate.

Pentru protecţia fişierelor sistemul de operare Windows, ediţiile Ultimate şi Enterprise, pune la dispoziţia utilizatorilor BitLocker Drive Encryption. Pentru protecţia fişierelor stocate pe medii amovibile de tipul hard disk urilor externe sau USB flash drive se foloseşte BitLocker To Go.

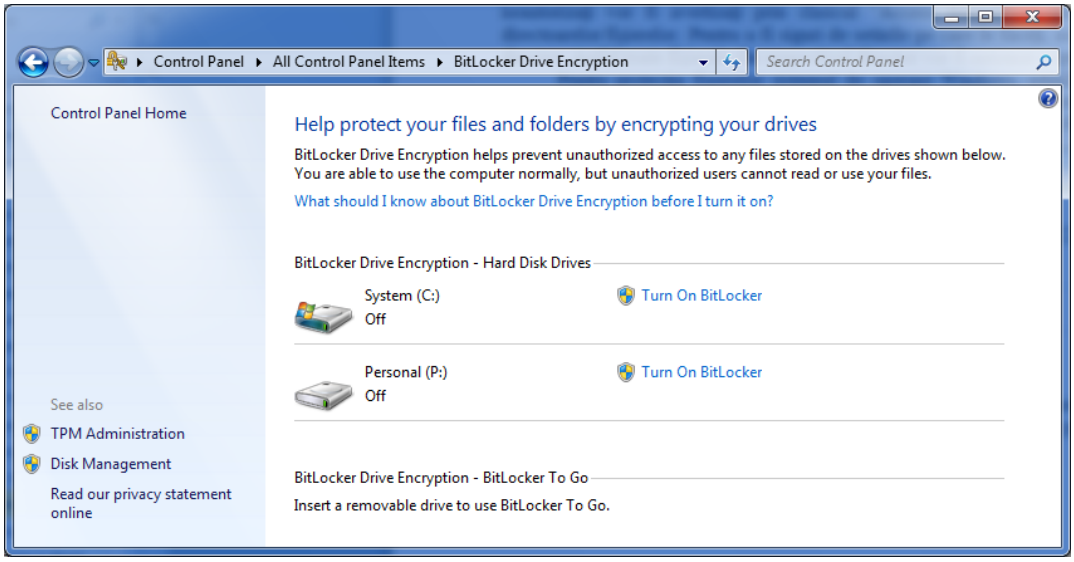

Control Panel ▸ All Control Panel Items ▸ BitLocker Drive Encryption
Search Control Panel
Control Panel Home
Help protect your files and folders by encrypting your drives
BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives shown below.
You are able to use the computer normally, but unauthorized users cannot read or use your files.
What should I know about BitLocker Drive Encryption before I turn it on?
BitLocker Drive Encryption - Hard Disk Drives
System (C:)
Off
Turn On BitLocker
Personal (P:)
Off
Turn On BitLocker
See also
TPM Administration
Disk Management
Read our privacy statement online
BitLocker Drive Encryption - BitLocker To Go
Insert a removable drive to use BitLocker To Go.

Figura nr. 7.4 – *Fereastra de criptare a discurilor*

Spre deosebire de EFS care criptează fişiere/directoarele individuale, BitLocker criptează un disc în totalitate. Menționăm că ori de câte ori se copiază un fişier de pe un drive criptat pe unul necriptat, fişierele vor fi decriptate pe noul disc, dar accesul la discul criptat cu BitLocker nu se poate realiza daca nu exista cheia de decriptare.

Totuşi este demonstrat că în anumite condiții, hardiscurile criptate pot fi decriptate mai ales când nu se respectă procedurile corecte de închidere deschidere a laptopurilor. Într-o demonstrație cu public, specialistul în Securitate Andy Malone a reuşit să decripteze un astfel de harddisk 39.

Cunoaşterea sistemului de fişiere este importantă prin prisma informațiilor ce le oferă despre data şi timpul creării şi accesării informațiilor

- *Copierea unui fişier dintr-o director al unei partiții FAT într-un alt director al aceleeaşi partiții, vă păstra aceeaşi dată şi oră a modificării dar va schimba data creării şi timpul la momentul realizării acțiunii*
- *Mutarea unui fişier dintr-o director al unei partiții FAT într-un alt director al aceleeaşi partiții, va păstra aceeaşi dată şi timp al modificării dar şi al creării*
- *Copierea unui fişier dintr-o director al unei partiții FAT într-un director al unei partiții NTFS va psătra aceeaşi dată şi timpă a modificării dar va modifica data şi timpul creării la momentul realizării acțiunii.*
- *Mutarea unui fişier dintr-o director al unei partiții FAT într-un director al unei partiții NTFS va psătra data şi timpul modificării şi creării.*
- *Copierea unui fişier dintr-o director al unei partiții NTFS într-un alt director al aceleeaşi partiții, va păstra aceeaşi dată şi timp a modificării dar va schimba data creării şi timpul la momentul realizării acțiunii.*
- *Mutarea unui fişier dintr-o director al unei partiții NTFS într-un alt director al aceleeaşi partiții va păstra aceeaşi dată a modificării şi timpul precum şi aceeaşi dată a creării şi timpul.*
- *Data modificări şi timpul unui fişier nu se modifică atât timp cât nu se modifică o proprietate a fişierului. Data creării şi timpul se vor modifica indiferent dacă fişierul a fost copiat sau mutat*

[39] http://www.chip.ro/review/windows/15842-cat-de-sigur-e-bitlocker

Gestiunea spațiului de pe volume

Utilizarea spațiului de pe volumele NTFS poate fi controlată prin activarea opțiunii *Disk Quotas*. Pentru administratori această facilitate este de un real folos dacă ne gândim la disponibilitatea sistemului.

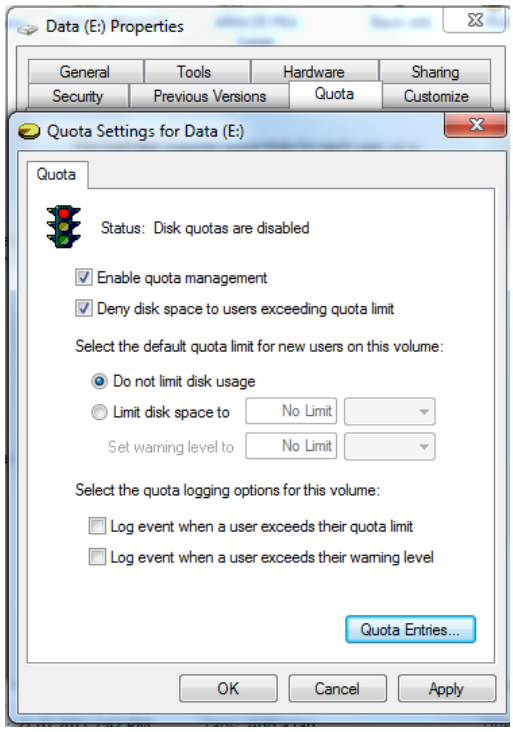


Figura nr. 7.5 – *Fereastra disk Quota*

Spațiul pe care fișierele le ocupă pe disc vor fi evidențiate pentru fiecare utilizator în parte, gestionarea sa făcându-se independent de localizarea fizică a fișierelor.

Activarea acestei opțiuni se face prin click dreapta pe un volum → Properties → Quota.

Compresia fișierelor

Fără a intra prea mult în amănunte spunem doar că algoritmul de compresie a fișierelor suportă clustere de până la 4KB. Dincolo de această dimensiune fișierele nu mai pot fi compresate. Cum funcționează compresia oferită de NTFS? Dacă accesați un fișier compresat, decompresia are în vedere doar porțiunea din fișier care trebuie citită. Această zonă este copiată în memoria calculatorului unde va fi ulterior modificată. În momentul în care părăsiți fișierul, datele din memorie vor fi scrise pe disc în format compresat.

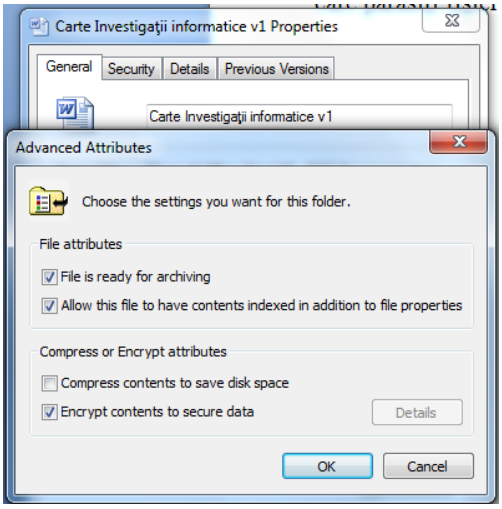


Figura nr. 7.6 - *Compresia şi/sau criptarea fişierelor*

Accesarea acestei facilităţi se face prin click dreapta pe directorul/fişierul pe care doriţi să-l compresaţi şi alegerea opţiunii *Properties*. Dacă vă plictiseşte lucrul cu mouse-ul puteţi apela la un utilitar care se lansează din linia de comandă: *compact.exe*.

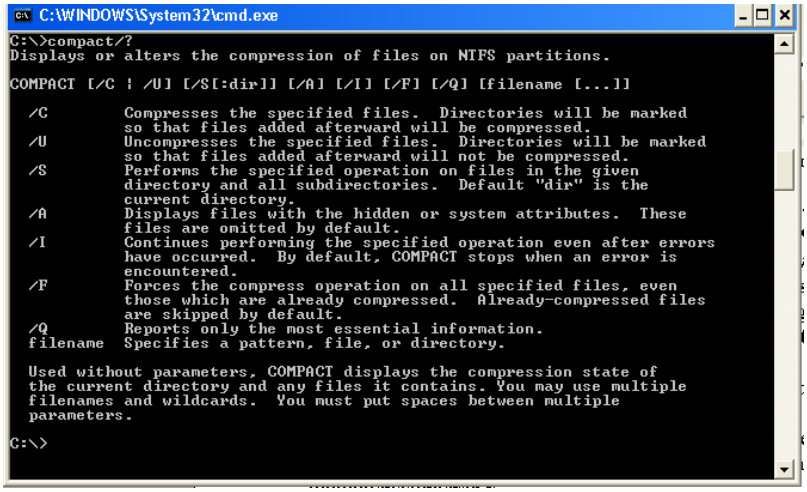

C:\WINDOWS\System32\cmd.exe
C:\>compact/?
Displays or alters the compression of files on NTFS partitions.
COMPACT [/C | /U] [/S[:dir]] [/A] [/I] [/F] [/Q] [filename [...]]
/C Compresses the specified files. Directories will be marked so that files added afterward will be compressed.
/U Uncompresses the specified files. Directories will be marked so that files added afterward will not be compressed.
/S Performs the specified operation on files in the given directory and all subdirectories. Default "dir" is the current directory.
/A Displays files with the hidden or system attributes. These files are omitted by default.
/I Continues performing the specified operation even after errors have occurred. By default, COMPACT stops when an error is encountered.
/F Forces the compress operation on all specified files, even those which are already compressed. Already-compressed files are skipped by default.
/Q Reports only the most essential information.
filename Specifies a pattern, file, or directory.
Used without parameters, COMPACT displays the compression state of the current directory and any files it contains. You may use multiple filenames and wildcards. You must put spaces between multiple parameters.
C:\>

Figura nr. 7.7 - *Comanda compact*

„Montarea" discurilor

Ne cerem scuze pentru barbarismul folosit, dar altă traducere pentru englezescul *mounted* nu am găsit. La ce se referă această facilitate? Este vorba de alocarea unui nume sau atribuirea unei etichete unui director de pe disk. Funcţionarea este identică cu atribuirea de litere partiţiilor create. Marele avantaj este că nu mai există limitarea impusă de folosirea doar a celor 26 de litere din alfabet.

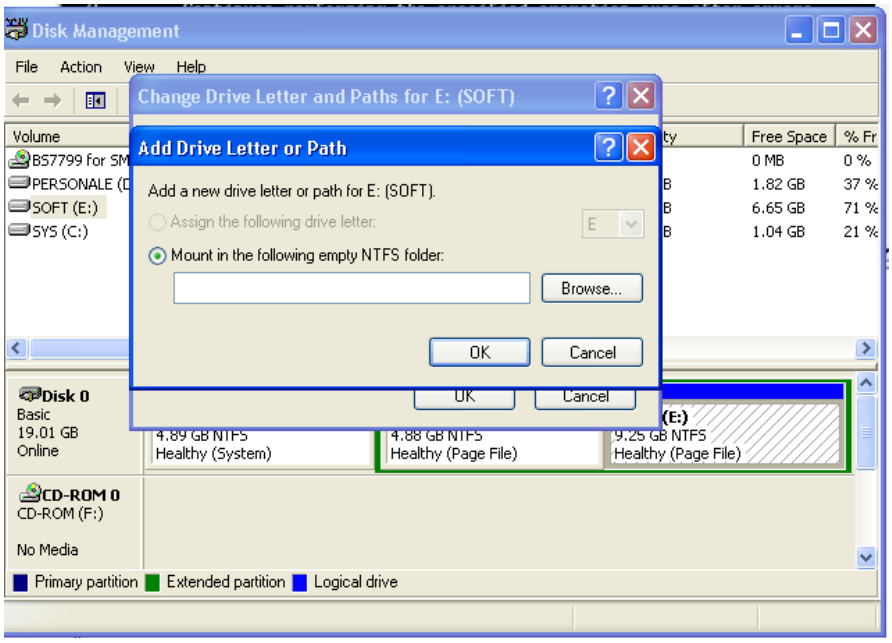


Figura nr. 7.8 - *Feresatra pentru montarea discurilor*

Se poate lucra fie din consola dedicată (*Start→Run→diskmgmt.msc*, sau din Control Panel*→Administrative Tools→Computer Management*) sau cu un utilitar lansat din linia de comandă: *mountvol.exe.*

Există o limitare a acestei facilități: cel care doreşte să monteze un volum trebuie să aibă permisiuni de administrator: să fie membru al acestui grup.

Servicii de indexare

Facilități ale NTFS-ului mai sunt, dar noi ne-am propus să vi le prezentăm pe cele mai folosite în practică. Prin urmare nu vom discuta despre hard links sau sparse file ci despre *indexare*.

Atunci când se doreşte regăsirea mai rapidă a documentelor de pe disc se poate apela la reorganizarea acestora cu ajutorul Serviciului de indexare. Funcționalitatea este similară bazelor de date sau căutării care se face cu ajutorul unui motor de căutare.

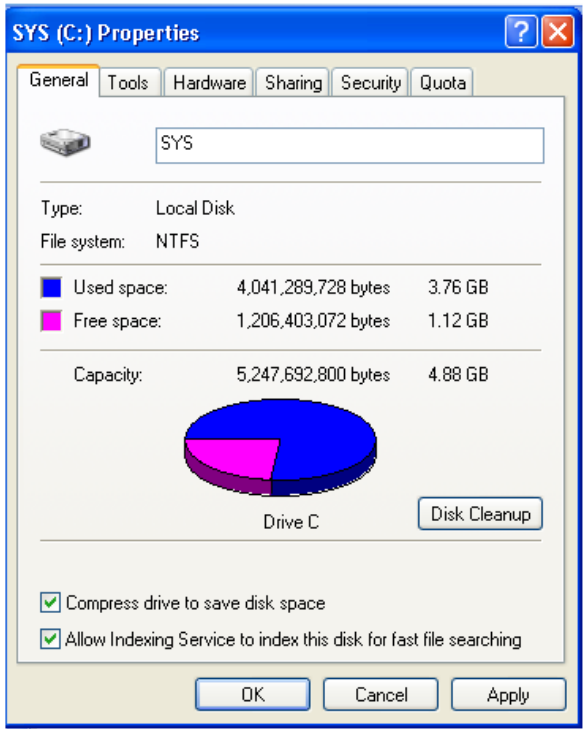


Figura nr. 7.9 – *Specificarea acțiunilor de indexare a fișierelor pe de un disc*

După prima indexare a unui volum, căutările ulterioare vor face apel la un jurnal în care sunt memorate modificările aduse fișierelor astfel încât numărul actualizarea indecșilor este proporțională cu numărul de fișiere modificate. Dacă nu folosiți această facilitate, de fiecare dată când apelați funcția de căutare, Windows-ul trebuie să deschidă fiecare fișier de pe disk, să caute informația dorită și apoi să închidă fișierul. Altfel spus, se *mișcă greu*.

Limitarea acestei facilități apare în momentul criptării: un fișier odată criptat va fi șters din lista de indecși.

Serviciul de indexare (**Error! Reference source not found.**) poate fi pornit și din *Control Panel→Administrative Tools→Computer Management→Indexing Service* (în Windows XP) și direct din Control Panel, Indexing Options în Windows 7.

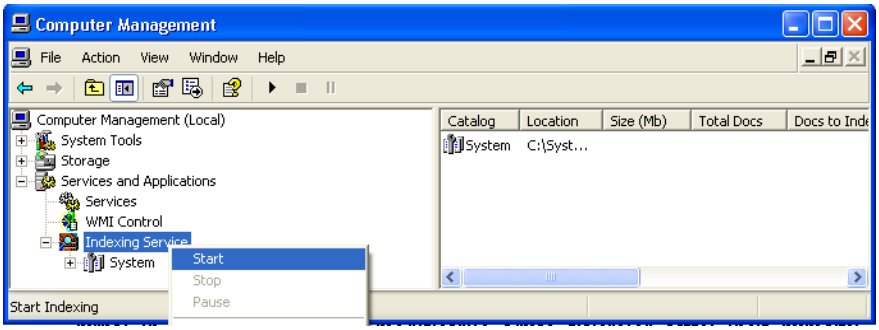


Figura nr. 7.10 – *Serviciile de indexare în Windows XP*

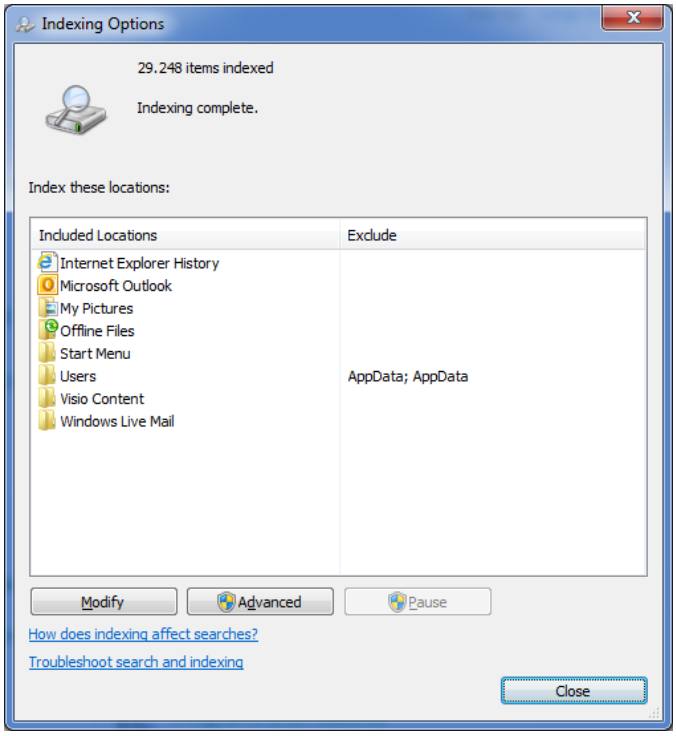


Figura nr. 7.11 – *Serviciul de indexare în Windows 7*

Nu vom încheia încă discuțiile legate de sistemul de fișiere (oricum vom mai face referire la acest subiect) fără a face o scurtă recapitulare a utilitarelor pe care le aveți la dispoziție în *\windows\system32*:

Utilitar	Funcționalitate
Cacls.exe	**Afișează și modifică ACL-urile asociate fișierelor sau directoarelor.**
Chkntfs.exe	**Afișează sau specifică când este programată verificarea automată a unui volum.**
Cipher.exe	**Afișează sau modifică informațiile cu privire la criptarea fișierelor/directoarelor de ve volumele NTFS.**
Compact.exe	**Afișează sau modifică compresia fișierelor/directoarelor de pe un volum NTFS.**
Convert.exe	**Convertește un volum/partiție din FAT în NTFS.**
Defrag.exe	**Reorganizarea fișierelor de pe disk.**
Expand.exe	**Extrage un fișier dintr-un format comprimat (de exemplu dintr-un .cab).**
Fsutil.exe	**Oferă mai multe opțiuni ce pot fi folosite în gestionarea sistemului de fișiere**
Mountvol.exe	**Folosit în managementul volumelor NTFS.**

Dacă doriți să aflați mai în detaliu informații despre calculatorul analizat, în modul comandă tastați *systeminfo*

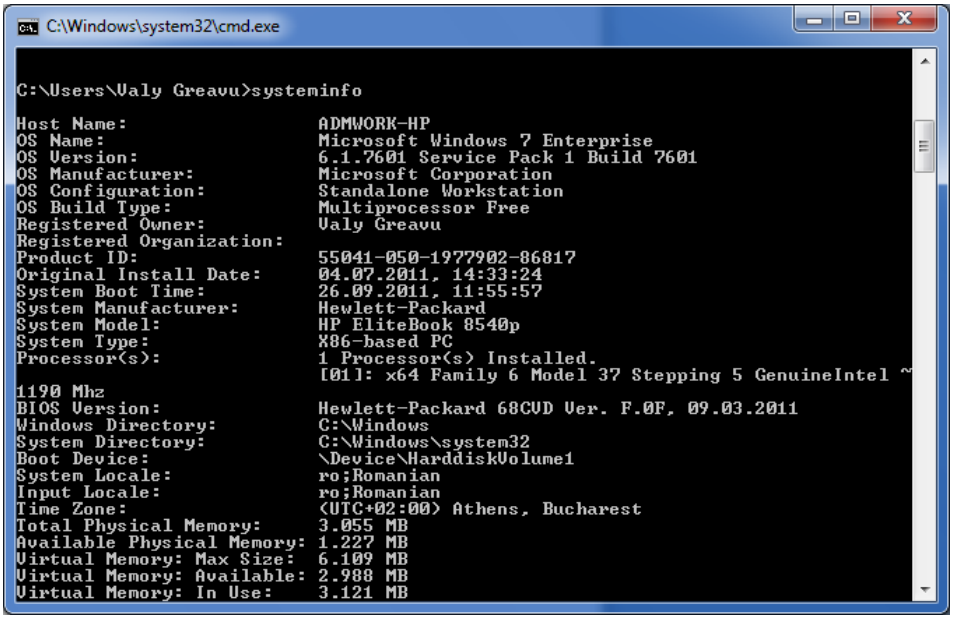

C:\Windows\system32\cmd.exe
C:\Users\Valy Greavu>systeminfo
Host Name: ADMWORK-HP
OS Name: Microsoft Windows 7 Enterprise
OS Version: 6.1.7601 Service Pack 1 Build 7601
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: Valy Greavu
Registered Organization:
Product ID: 55041-050-1977902-86817
Original Install Date: 04.07.2011, 14:33:24
System Boot Time: 26.09.2011, 11:55:57
System Manufacturer: Hewlett-Packard
System Model: HP EliteBook 8540p
System Type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x64 Family 6 Model 37 Stepping 5 GenuineIntel ~
1190 Mhz
BIOS Version: Hewlett-Packard 68CVD Ver. F.0F, 09.03.2011
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: ro;Romanian
Input Locale: ro;Romanian
Time Zone: (UTC+02:00) Athens, Bucharest
Total Physical Memory: 3.055 MB
Available Physical Memory: 1.227 MB
Virtual Memory: Max Size: 6.109 MB
Virtual Memory: Available: 2.988 MB
Virtual Memory: In Use: 3.121 MB

Figura nr. 7.12 – *Informații despre sistem în formatul linie de comandă*

7.2 Gestiunea Regiştrilor

Microsoft spune despre **Registry** că reprezintă o bază de date centralizată, cu o structură ierarhică, folosită la gestionarea informațiilor necesare configurării sistemului, aplicațiilor şi dispozitivelor hardware ale calculatorului[40]:

- **Subtree (Subarbore)** – Nivelul superior. Sunt 5 arbori în structură.
  - **Keys (Chei)**- Containere pentru subchei şi valori
    - **Subkeys (Subchei)**- Container pentru valori
      - **Values (Valori)**
        - **Data (Date)**

Ca structură, regiştrii sunt alcătuiți din mai multe containere care pot fi asimilate directoarelor clasice: *subtrees, keys* şi *subkeys.* Datele propriu-zise sunt stocate sub forma *intrărilor* care pot fi asimilate fişierelor clasice.

O *intrare* este alcătuită dintr-un *nume*, un *tip* de dată prin care este definită lungimea şi formatul datei pe care intrarea respectivă îl poate stoca şi o *valoare* care stochează data propriu-zisă.

Aplicațiile instalate pe calculator îşi păstrează datele sub forma intrărilor în regiştri. Prin urmare, **regiştri aparțin aplicațiilor şi nu utilizatorilor**. Modificarea setărilor regiştrilor fără cunoaşterea exactă a unei aplicații poate duce la *decesul* calculatorului!

[40] http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986

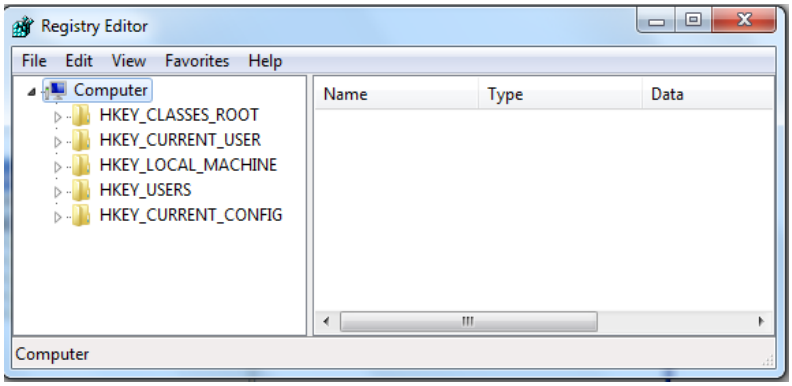


Figura nr. 7.13 – *Fereastra Registry Editor*

Primul subarbore este **HKEY_CLASSES_ROOT (**HKCR). Acesta este creat dinamic în momentul boot-ării şi conţine două tipuri de date:

- Date prin intermediul cărora se face asocierea între diferite tipuri de fişiere şi programele care le utilizează. Subcheile din HKCR au acelaşi nume ca şi extensiile fişierelor pentru respectivul tip de fişiere.
- Date pentru configurarea obiectelor COM, programelor. Subcheile folosesc ID-ul programului respectiv sau numele cheii părinte pentru alte clase de informaţii.

Informaţiile din acest subarbore sunt preluate din alte două *frunze:* HKEY_LOCAL_MACHINE\SOFTWARE\Classes respectiv HKEY_CURRENT_ USER\SOFTWARE\Classes

Cel de al doilea subarbore este **HKEY_CURRENT_USER (**HKCU). El conţine profilul utilizatorului logat pe calculator incluzând: variabilele de mediu, programele, setările desktop-ului, conexiunile reţelei, imprimantele şi personalizările la nivel de aplicaţii. În acestă frunză nu sunt memorate date propriu-zise ci doar pointeri către identificatorul de securitate corespunzător utilizatorului curent (HKEY_USERS\Security ID).

De fiecare dată când se loghează un alt utilizator pe calculator se creează o nouă HKCU. Datele pentru acest subarbore vor fi preluate din profilul utilizatorului curent. Dacă nu este găsit nici un profil, subraborele este creat pornind de la setările din profilul utilizatorului implicit (default): *C:\Users\Default\Ntuser.dat*.

Al treilea subarbore şi poate cel mai important este **HKEY_LOCAL_MACHINE (**HKLM) şi conţine informaţii despre configuraţia hardware a calculatorului local precum şi informaţii despre sistemul de operare: tipul busului, memoria existentă, drivere, parametrii de control la startare etc.

La rândul său acest subarbore conţine cinci chei: HARDWARE, SAM, SECURITY, SOFTWARE şi SYSTEM.

Cheia HARDWARE păstrează datele cu privire la componentele hardware pe care le detectează calculatorul şi este recreată la fiecare pornire a computerului. sunt incluse aici informaţii despre toate dispozitivele, driverele acestora şi celelalte resurse al computerului.

Cheia SAM conţine informaţiile folosite de managerul pentru securitate (SAM – Security Account Manager). Pentru serverele Windows care nu au rol de controlere de domeniu, această cheie este folosită pentru a memora informaţiile despre utilizatori sau grupurile de utilizatori. În cazul controlerelor de domeniu, acest informaţii sunt stocate în Active Directory.

Informaţiile cu privire la securitatea sistemului şi a reţelei sunt stocate în cheia SECURITY. Subcheia HKLM\SECURITY\SAM păstrează o dublură a informaţiilor din subcheia SAM. Informaţiile din această cheie sunt prezentate în format binar şi nu pot fi editate!

Subcheia SOFTWARE este cea care păstrează variabilele asociate programelor instalate pe calculator (inclusiv producătorul) şi care se aplică utilizatorilor

Subcheia HKLM\SYSTEM păstrează intrările specifice set de control curent sau celelalte seturi de control utilizate. Trebuie să existe cel puţin două seturi de control pentru startarea sistemului.

Cel de al patrulea subarbore, **HKEY_USERS (**HKU) conţine toate profilurile utilizatorilor activi pe calculatorul respectiv, şi include cel puţin trei subchei:

- DEFAULT – păstrează profilul utilizat atunci când nu există nici un utilizator logat (când este afişat promptul pentru login)
- O subcheie al cărui nume începe cu S şi care face referire la SID-ul (identificatorul de securitate) utilizatorului local. Conţine informaţii despre profilul utilizatorului curent. Datele din această cheie apar şi în HKCU.
- O subcheie al cărui nume începe cu S şi se termină cu *Classes*.

În Windows 7, profilul utilizatorului implicit nu este memorat în regiştri ci pe discul pe care este instalat SO, în C:*Users\Default\Ntuser.dat.*

Ultimul arbore din această prezentare este **HKEY_CURRENT_CONFIG (HKCC)** şi păstrează datele despre configuraţia hardware corespunzătoare profilului curent. De fapt acest subarbore conţine un pointer către subcheia HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles. subkey. Este folosit pentru a uşura accesul la date.

Pentru ca modificările efectuate asupra regiştrilor să producă efecte este nevoie de log off, restartarea serviciului afectat sau chiar a Windows-ului. În general, dacă schimbările au avut loc în subcheia *CurrentControlSet*, calculatorul va trebui să fie repornit. Dacă aţi modificat valori din arborele HKEY_CURRENT_USER va trebui să părăsiţi sesiunea de lucru (log off) şi să faceţi login din nou pentru ca modificările să aibă efect.

La oprirea calculatorului, majoritatea informaţiilor din regiştri sunt memorate pe hard disk în *windows\system32\config* sub forma unor fişiere (fără extensie) numite *hive*:

- *sam* (HKEY_LOCAL_MACHINE\SAM)
- *security* (HKEY_LOCAL_MACHINE\SECURITY)
- *software* (HKEY_LOCAL_MACHINE\SOFTWARE)
- *system* (HKEY_LOCAL_MACHINE\SYSTEM)
- *default* (HKEY_USERS\DEFAULT).

Pentru a asigura integritatea sistemului, aceste fişiere sunt protejate împotriva oricăror acţiuni on-line. În acelaşi director există copii de siguranţă ale acestor fişiere create în mod automat după log on în directorul RegBack precum şi evidenţa schimbărilor care au avut loc (extensia *.log*).

Tot pentru a asigura funcţionarea corectă a calculatorului se recomandă efectuarea copiilor de siguranţă ale regiştrilor Windows prin exportul acestora. În mod automat regiştrii sunt salvaţi la realizarea copiilor de tip System Restore.

Salvarea manuală sau particularizată se poate efectua după următoarea procedură:

1. Se deschide Regedit în mod administrativ
2. Se alege de exemplu clasa HKEY_Local_Machine
3. Din meniul File se alege opţiunea Export
4. Se specifică locaţia de salvare a fişierului cu extensia Reg.

Fiind una din cele mai sensibile componente ale unui sistem de operare Windows, trebuie să fim foarte atenţi cu permisiunile pe cheile de regiştri pentru că majoritatea atacurilor actuale la

integritatea sistemelor de calcul se bazează pe scrierea de chei în regiştri, transformând calculatorul într-un instrument controlabil de la distanță de hackeri.

7.3 Validarea şi discriminarea datelor

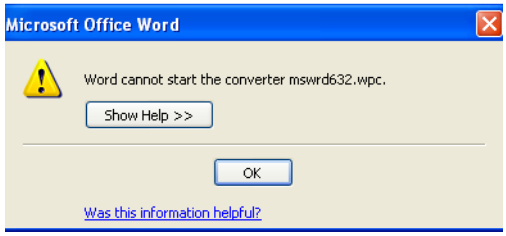
Două aspecte sunt critice pentru orice investigator: *integritatea datelor copiate* (validarea acestora) *respectiv discriminarea datelor* (sortarea şi căutarea prin datele investigate). Producătorii de aplicații pentru investigații informatice pun la dispoziție trei componente care răspund acestor deziderate:

- Hashing
- Filtrare
- Analiza antetului fişierelor

Validarea datelor se realizează prin calcularea unor valori *hash* asupra unui text, fişier sau întregului conținut al unui hard disk. În limbaj tehnic se mai întâlnesc variantele cifra de control (checksum) sau hash code. Aceste valori folosesc la identificarea fişierelor duplicate sau pentru a verifica dacă o imagine sau o clonă folosită în investigații a fost realizată cu succes.

O organizație poate crea o listă valori hash pentru instalările de sisteme de operare, aplicații sau documente. În cazul unei investigații aceste valori vor fi ignorate analiza concentrându-se doar asupra fişierelor care nu apar pe această listă. În situația în care nu există o astfel de listă se poate face apel la National Software Reference Library[41] de unse se poate descărca o astfel de listă. Software-ul de investigații FTK preia în mod automat valorile hash ale fişierelor din lista menționată anterior.

O situația cu care ne putem confrunta este cea în care dorim să verificăm exactitatea unui fişier. De exemplu, pe un hard disk am identificat fişierul *Auditat.doc* ca fiind suspect. În momentul în care dorim să îl deschidem, aplicația asociată acestei extensii (Microsoft Office) va produce mesajul de eroare din figura de mai jos.



Vom analiza acelaşi fişier cu ajutorul WinHex pentru că vrem să ne asigurăm că acel fişier este chiar unul de tip document.

[41] http://www.nsrl.nist.gov/Project_Overview.htm

Fişierul este de fapt o imagine (are extensia .jpg nu .doc cum apare pe disc)

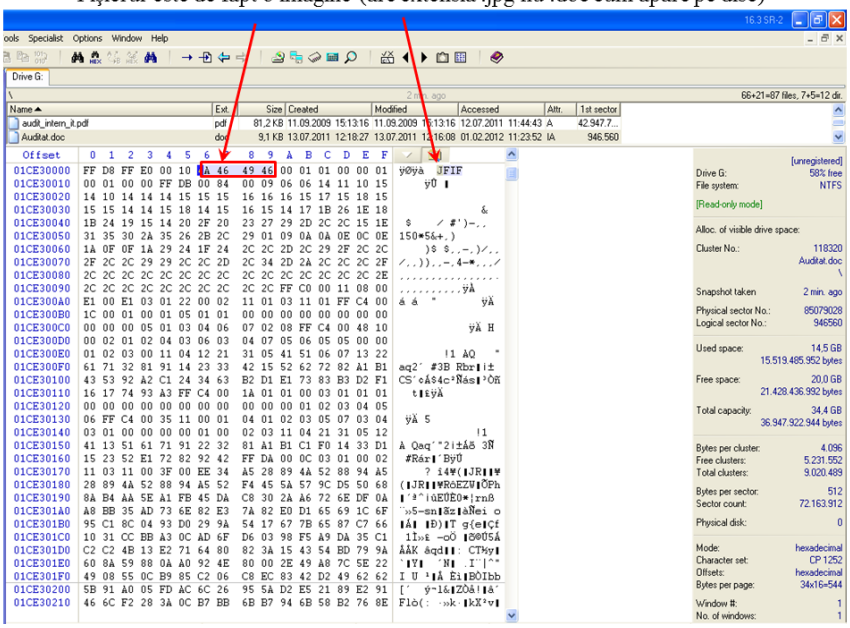


Figura nr. 7.14 – *Determinarea corectă a tipului unui fişier*

De unde ştim că are extensia *.jpeg?* Ceea ce afişează WinHex în headerul fişierului în imaginea de mai sus – JFIF, este acronimul pentru **JPEG File Interchange Format** (dacă ar fi fost un fişer de tip doc, în hexazecimal extensia ar foi fost reprezentată sub forma D0 CF 11 E0 A1 B1 1A E1 00). În practică sunteţi scutiţi de astfel de artificii deoarece majoritatea aplicaţiilor profesionale folosite în investigaţii analizează antetul fişierelor şi nu extensia acestora.

7.4 Protecţia/blocarea la scriere

Principala preocupare a investigatorului este de a asigura un mediu de lucru care să nu modifice în nici un fel sistemul analizat compromiţând astfel integritatea dovezii. În primul rând trebuie să ne asigurăm că în momentul în care conectăm dispozitivul de stocare a datelor la calculator folosit ca instrument pentru investigare, acesta din urmă nu va produce modificară asupra datelor sursă.

În momentul în care conectăm un astfel de dispozitiv la calculator se modifică fişierul de configurare a acestuia cu data şi ora ultimei accesări.

Mecanismele de protejare la scriere (write blocker) pot fi atât hardware cât şi software. Mecanismele hardware permit conectarea directă a dispozitivului care conţine probele şi pornirea calculatorului în mod normal, independent de sistemul de operare rulat. Acest tip de mecanisme se recomandă mai ales în cazul utilizării aplicaţiilor pentru investigaţii bazate pe interfeţe grafice

Evităm a nominaliza prea mulţi astfel de producători dintr-un simplu motiv: piaţa este dinamică şi echipamente noi apar în fiecare zi.

Mecanismele software, de multe ori, sunt proiectate pentru un anumit sistem de operare. Piaţa pune o mulţime de aplicaţii în acest sens, comerciale sau gratuite[42]. Discuţia este ceva mai complicată pentru că ne putem întâlni în practică cu două situaţii: colectarea probelor trebuie să se realizeze la locul infracţiunii; sau colectarea probelor se poate face la sediul investigatorului. În

[42] SEIF Block http://www.winsite.com/Utilities/Disk-Utilities/SAFE-Block/

primul caz este de dorit să se diminueze hardware-ul ce trebuie deplasat la locul infracțiunii şi se preferă utilizarea unui laptop. În cel de al doilea caz este posibil să se prefere achiziționarea unei stații dedicate acestui scop, cu cât mai multe extensii posibile. Modul cum se configurează o stație pentru investigați depinde de experiența şi preferințele profesionistului.

În cazul sistemelor Windows blocarea scrierii pe dispozitive externe de stocare a datelor poate fi realizată direct din regiştrii calculatorului

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect. În cazul în care această cheie nu există, va fi creată de investigator, astfel:

1. Se deschide Registry Editor (Run > regedit)
2. Se navighează până la HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
3. Se creează o cheie nouă (Edit > New > Key) pe care o denumim StorageDevicePolicies
4. În această cheie se creează o nouă valoare DWORD (32-bit) (Edit > New > DWORD (32-bit) value) pe care o denumim WriteProtect
5. Dublu click pe WriteProtect şi setăm Value Data 1 ca în imaginea de mai jos. Implicit aceasta are valoarea 0.

Imaginea de mai jos arată crearea valorii WriteProtect şi modificarea acesteia pentru a bloca scrierea.

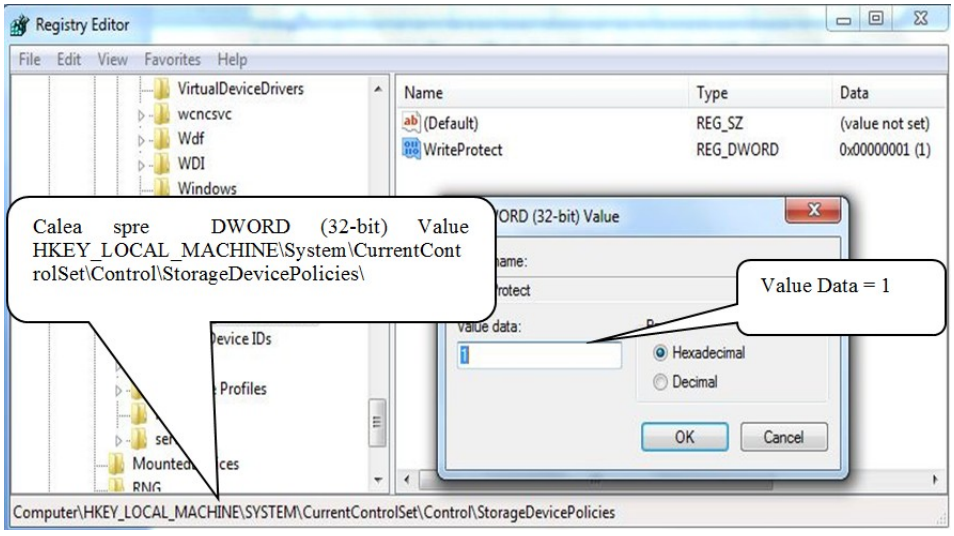


Figura nr. 7.15 – *Blocarea la scrierea pe dispozitive de stocare*

Mediile de stocare folosite pentru achiziția datelor trebuie să fie reformatate şi verificate împotriva viruşilor. Puteți folosi ProDiscover[43] *sau SecureClean*[44].
Nu uitați: trebuie să asigurați controlul tuturor probelor şi să documentați orice acțiune întreprinsă în timpul examinării!

[43] http://www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14
[44] http://www.whitecanyon.com/secureclean-update.php

Capitolul 8. Poşta electronică (e-mail)

Despre fişiere şi modul de analizare a acestora vom mai discuta pe parcurs. Probele pe care le pot conține mesajele transmise prin intermediul poştei electronice sunt însă la fel de importante. Să menționăm doar mesajele tip „phising[45]" care au proliferat în ultimul timp.

8.1 Client, server şi mesaj

Probabil că astăzi puțin sunt cei care nu folosesc poşta electronică în activitățile cotidiene. Accesat de pe un calculator sau dispozitiv portabil, mailul a ajuns critic pentru activitățile economice ale companiilor. Putem transmite şi recepționa mailuri în două situații: prin Internet, folosind un server public; prin intranet (rețeaua privată a organizației) folosind un server ce nu este administrat de un furnizor de servicii de comunicații electronice ci de organizația în care muncim.

În ambele situații serverul este cel pe care rulează programul specializat pe o astfel de sarcină (Microsoft Exchange, Group Wise, Sendmail). Calculatoarele pot accesa acest serviciu fie direct din browser fie folosind un soft specializat denumit „client de email": Microsoft Outlook, Lotus etc.

Indiferent de sistemul de operare, de serverul de mail sau de aplicația client folosite, un utilizator îşi poate accesa poşta electronică în funcție de permisiunile primite de la administratorul acelui sistem.
Nu trebuie să uităm că emailul de serviciu este un bun privat al companiei în timp ce emailul personal este folosit de către un furnizor public!
Tot ce urmează după simbolul „@" în adresa/numele utilizatorului este folosit pentru a identifica domeniul care pune la dispoziție acest serviciu. Fără a intra în detalii juridice, accesarea contului pus la dispoziție de către o organizație privată nu se va considera violare de corespondență.

Investigarea mailurilor organizaționale este o sarcină ceva mai facilă deoarece se foloseşte o denumire standardizată a numelui utilizatorilor şi identificarea acestora nu este greu de înfăptuit.

Cum în universul IT cam toate lucrurile sunt standardizate, nici poşta electronică nu face excepție. **RFC 5322**[46] este standardul care stabileşte Internet Message Format (IMF) şi sintaxa mesajelor ce sunt transmise între utilizatori. Un e-mail conține, confirm specificațiilor RFC 5322:

- antetul (header);.
- corpul (body), textul mesajului propriu-zis.

Antetul la rândul său conține:

- expeditor (From) - adresa de e-mail a expeditorului mesajului (numele unui expeditor poate fi falsificat);
- destinatar (To) - adresa de e-mail a destinatarului (sau adresele destinatarilor, dacă sunt mai mulți);

[45] Phishing (înşelăciunea) reprezintă o formă de activitate infracțională care constă în obținerea unor date confidențiale, cum ar fi date de acces pentru aplicații de tip bancar, aplicații de comerț electronic (ca eBay sau PayPal) sau informații referitoare la carduri de credit, folosind tehnici de manipulare a datelor identității unei persoane sau a unei instituții. (Sursa: http://ro.wikipedia.org/wiki/Phishing)
[46] http://tools.ietf.org/html/rfc5322

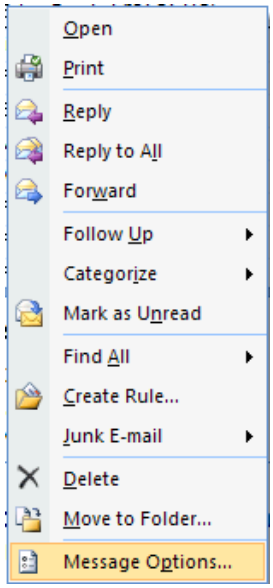
- subiectul (Subject) - un rezumat al mesajului; data (Date) - data şi ora locală a trimiterii mesajului.
- Cc - copie la indigo (de la "Carbon Copy") - o copie identică a mesajului trebuie trimisă şi la adresa sau adresele de e-mail din acest câmp;
- Bcc - copie la indigo oarbă (de la "Blind Carbon Copy") - la fel ca şi Cc, doar că nici un destinatar nu va afla la cine se mai trimit copii ale mesajului, în afară de el însuşi.

8.2 Examinarea mesajelor

Presupunem că o anumită infracțiune a fost realizată folosind ca instrument e-mailul. Sau nu, dar ca investigator trebuie să analizezi toate probele identificate la locul infracțiunii. Trebuie deci accesat calculatorul pentru a recupera o astfel de probă şi pentru a analiza antetul mesajului: acolo sunt informații care pot să conducă investigatorul către suspect.

Cu ceva ani în urmă ni s-a cerut opinia cu privire la un schimb de mesaje din cadrul unei organizații. Din nefericire pentru cel incriminat probele nu erau digitale, ci *doar* sub formă de tipăritură. Aşa ceva nu este corect. Este nevoie de ambele variante.

În Microsoft Office Outlook 2007, antetul unui mesaj poate fi vizualizat printr-un simplu click dreapta al mouse-ului pe mesajul analizat (nu vom prezenta acest subiect pentru fiecare versiune de Outlook. Aceste informații sunt uşor de aflat dacă se cunoaşte versiunea aplicației client e-mail. Pentru a ştii exact ce se foloseşte, dacă aplicația este pornită se accesează meniul Help, opțiunea About):



Ulterior sistemul va afişa:

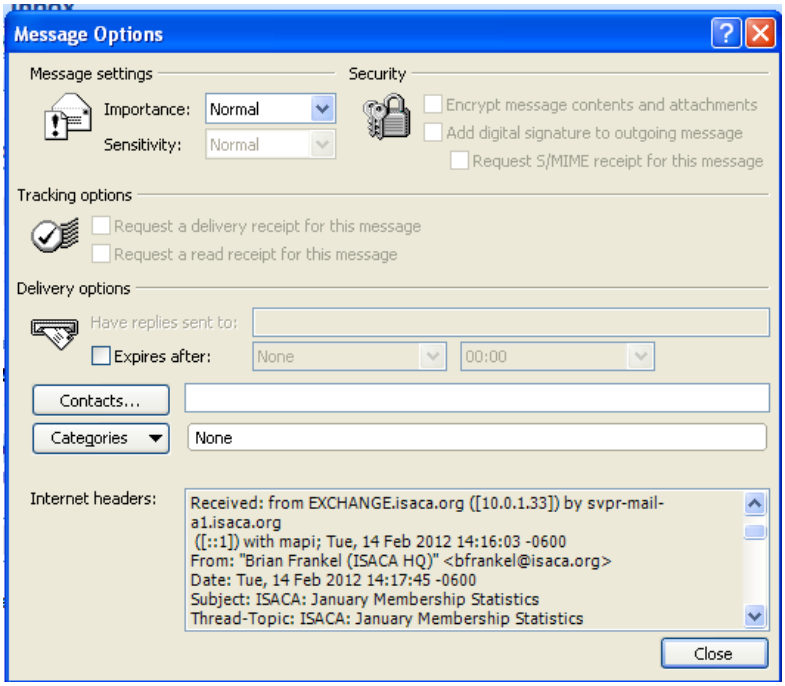


Figura nr. 8.1- *Opțiunile unui mesaj electronic în Microsoft Office Outlook*

Pentru un mail folosind serviciul public Google, antetul va fi vizibil dacă se activează opțiunea „Afișați originalul”

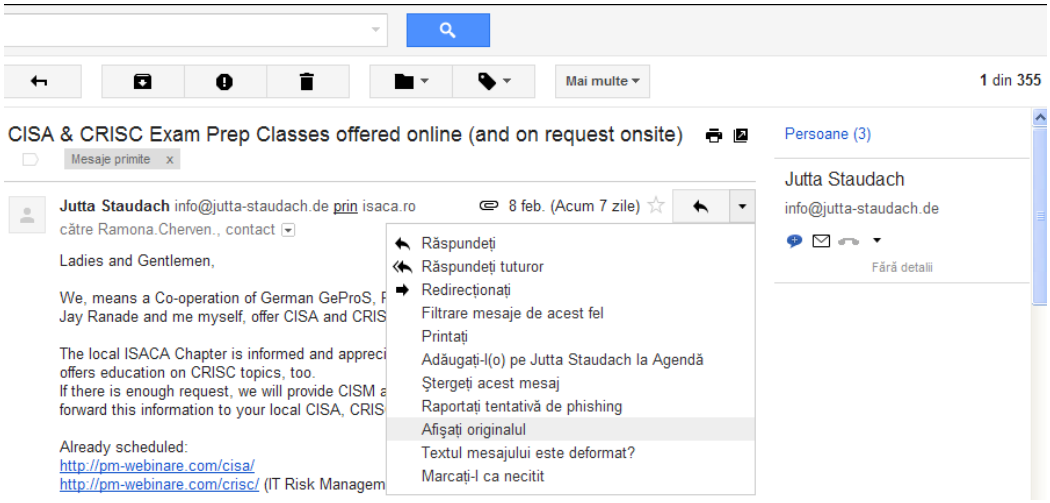

Mai multe
1 din 355
CISA & CRISC Exam Prep Classes offered online (and on request onsite)
Mesaje primite
Jutta Staudach info@jutta-staudach.de prin isaca.ro
8 feb. (Acum 7 zile)
către Ramona.Cherven., contact
Ladies and Gentlemen,
We, means a Co-operation of German GeProS,
Jay Ranade and me myself, offer CISA and CRIS
The local ISACA Chapter is informed and appreci
offers education on CRISC topics, too.
If there is enough request, we will provide CISM
forward this information to your local CISA, CRIS
Already scheduled:
http://pm-webinare.com/cisa/
http://pm-webinare.com/crisc/ (IT Risk Managem
Răspundeți
Răspundeți tuturor
Redirecționați
Filtrare mesaje de acest fel
Printați
Adăugați-l(o) pe Jutta Staudach la Agendă
Ștergeți acest mesaj
Raportați tentativă de phishing
Afișați originalul
Textul mesajului este deformat?
Marcați-l ca necitit
Persoane (3)
Jutta Staudach
info@jutta-staudach.de
Fără detalii

Figura nr. 8.2 – *Afişarea opţiunilor unui mesaj de e-mail în Gmail*

În acest caz, pe lângă mesajul propriu-zis vor fi afişate şi informaţiile din antetul mesajului:

Delivered-To: adrian.munteanu@isaca.ro
Received: by 10.204.118.16 with SMTP id t16csp33610bkq;
Wed, 8 Feb 2012 03:58:24 -0800 (PST)
Received: by 10.152.148.106 with SMTP id tr10mr15613344lab.41.1328702303765;
Wed, 08 Feb 2012 03:58:23 -0800 (PST)
Return-Path: <board+bncC0aWp7KkCBDUxsn5BBoEgti4pQ@isaca.ro>
Received: from mail-lpp01m010-f69.google.com (mail-lpp01m010-f69.google.com [209.85.215.69])
by mx.google.com with ESMTPS id tu6si5106241lab.2.2012.02.08.03.58.13
(version=TLSv1/SSLv3 cipher=OTHER);
Wed, 08 Feb 2012 03:58:22 -0800 (PST)
Received-SPF: pass (google.com: domain of board+bncC0aWp7KkCBDUxsn5BBoEgti4pQ@isaca.ro designates 209.85.215.69 as permitted sender) client-ip=209.85.215.69
Authentication-Results: mx.google.com; spf=pass (google.com: domain of board+bncC0aWp7KkCBDUxsn5BBoEgti4pQ@isaca.ro designates 209.85.215.69 as permitted se
Received: by lahm13 with SMTP id m13sf1129761lah.0
for <multiple recipients>; Wed, 08 Feb 2012 03:58:13 -0800 (PST)
Received: by 10.213.25.68 with SMTP id y4mr1306744ebb.3.1328702292869;
Wed, 08 Feb 2012 03:58:12 -0800 (PST)
X-BeenThere: board@isaca.ro
Received: by 10.213.3.210 with SMTP id 18ls291493ebo.1.gmail; Wed, 08 Feb 2012
03:58:12 -0800 (PST)
Received: by 10.213.3.136 with SMTP id 8mr2068770ebn.11.1328702292268;
Wed, 08 Feb 2012 03:58:12 -0800 (PST)
X-BeenThere: contact@isaca.ro
Received: by 10.14.119.133 with SMTP id n51s3349854eeh.0.canary; Wed, 08 Feb
2012 03:58:12 -0800 (PST)
Received: by 10.213.33.8 with SMTP id f8mr4109902ebd.119.1328702291916;
Wed, 08 Feb 2012 03:58:11 -0800 (PST)
Received: by 10.213.33.8 with SMTP id f8mr4109900ebd.119.1328702291812;
Wed, 08 Feb 2012 03:58:11 -0800 (PST)
Received: from mxout004.mail.hostpoint.ch (mxout004.mail.hostpoint.ch. [217.26.49.183])
by mx.google.com with ESMTPS id y56si826769eef.184.2012.02.08.03.58.11
(version=TLSv1/SSLv3 cipher=OTHER);
Wed, 08 Feb 2012 03:58:11 -0800 (PST)
Received-SPF: neutral (google.com: 217.26.49.183 is neither permitted nor denied by best guess record for domain of info@jutta-staudach.de) client-ip=217.26

Figura nr. 8.3 – *Detaliile unui mesaj de e-mail*

Revenind la figură, dacă selectăm textul şi îl vom copia într-un editor (Word, Notepad) putem obține următoarele informații

```
Received: from EXCHANGE.isaca.org ([10.0.1.33]) by svpr-mail-
a1.isaca.org
 ([::1]) with mapi; Tue, 14 Feb 2012 14:16:03 -0600
```

Această informație ne spune că mesajul a fost transferat în data de 14 februarie 2012 ora 14:16:03 Pacific Standard Time (“-0600” se presupune ora GMT)

```
From: "Brian Frankel (ISACA HQ)" bfrankel@isaca.org
```

Acesta este expeditorul mesajului

```
Date: Tue, 14 Feb 2012 14:17:45 -0600
```

Data şi ora la care a fost transmis mesajul conform ceasului de pe calculatorul expeditorului

```
Subject: ISACA: January Membership Statistics
```

Acesta este subiectul mesajului

```
Thread-Topic: ISACA: January Membership Statistics
Thread-Index: AczrVbZNtS5GH8HyQJC4HNPd+plrMQ==
```

Această informație este folosită pentru a asocia mai multe mesaje cu acelaşi subiect.

```
Message-ID:
47566EA1E630D944AE2923C9B272100306C6FCCDB43B@EXCHANGE.isaca.org
```

Mesajului i se asociază un identificator de către serverul de mail. Informația este folsoită pentru a identifica mesajul pe serverul de mail de pe care a fost expediat.

```
-MS-Has-Attach: yes
```

Mailul are ataşat un fişier

```
MIME-Version: 1.0
```

Versiunea protocolului MIME[47] folosit

```
To: Undisclosed recipients:;
```

Această ăinformație ne spune că mesajul a fost transmis către mai mulți destinatari, dar adresele de mail ale acestora nu sunt afişate

```
Return-Path: bfrankel@isaca.org
```

Această informație ne indică adresa de mail a expeditorului

Programele client de e-mail salvează mesajele local sau le păstrează doar pe server, în funcție de modul de configurare a acestora.
În cazul Outlook, mesajele transmise, recepționate,şterse, schițele de mesaje sunt salvate într-un fişier .pst. Mesajele off line sunt salvate într-un fişier .ost (în cazul în care calculatorul nu este conectat la Internet)
În cazul sistemelor de e-mail web-based, mesajele sunt afişate şi salvate ca pagini web în memoria cache a browserului web.
Nu trebuie uitat că unii furnizori de poştă electronică oferă şi facilități de mesagerie electronică instantanee. În acest caz, serviciul poate salva conținutul mesajelor într-un format proprietar.

Dacă se doreşte studierea mesajelor trimise de la valy.greavu la adrian.munteanu in perioada 15 ianuarie 2012 si 15 februarie 2012 se va analiza jurnalul de pe serverul de mail:

[47] Multipurpose Internet Mail Extensions (MIME) este un standard ce extinde formatul unui mesaj de poştă electronică pentru a permite: seturi de caractere non ASCII; ataşamente, altele decât text; informații în header în set de caractere non ASCII

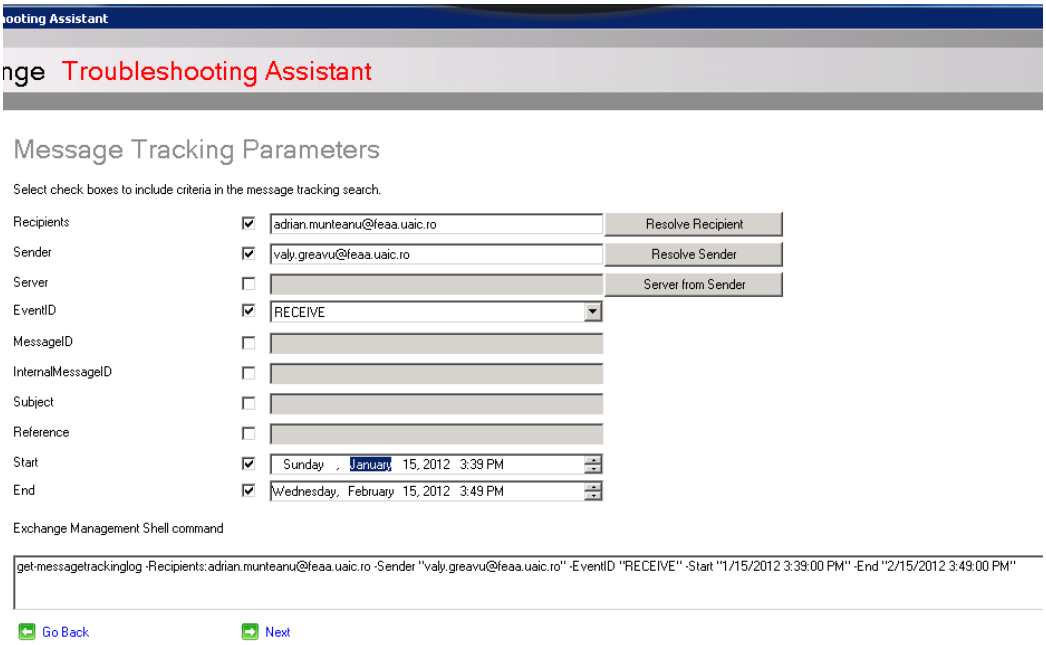
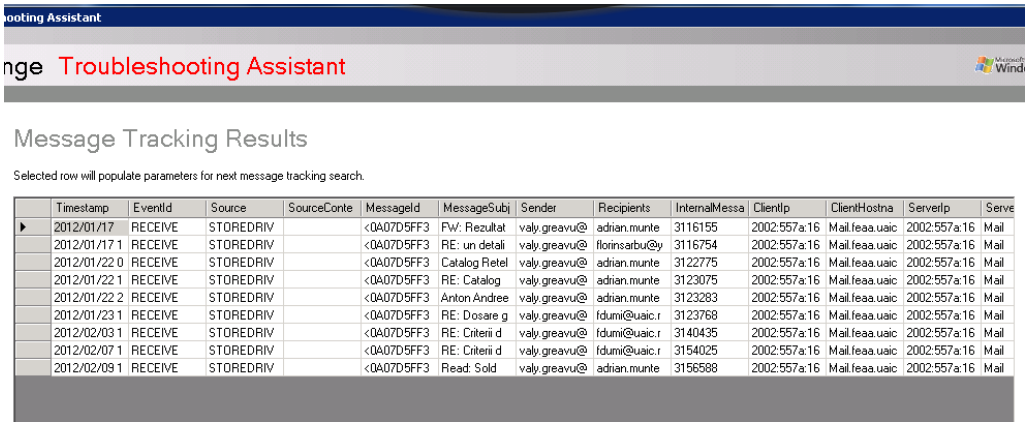


Figura nr. 8.4 – *Urmărirea mesajelor de pe un server de email Exchange*

Lista mesajelor trimise de la valy.greavu (sender) catre adrian.munteanu (recipient).


ooting Assistant
nge Troubleshooting Assistant
Message Tracking Results
Selected row will populate parameters for next message tracking search.

Timestamp	EventId	Source	SourceConte	MessageId	MessageSubj	Sender	Recipients	InternalMessa	ClientIp	ClientHostna	ServerIp	Serve
2012/01/17	RECEIVE	STOREDRIV		<0A07D5FF3	FW: Rezultat	valy.greavu@	adrian.munte	3116155	2002:557a:16	Mail.feaa.uaic	2002:557a:16	Mail
2012/01/17 1	RECEIVE	STOREDRIV		<0A07D5FF3	RE: un detali	valy.greavu@	florinsarbu@y	3116754	2002:557a:16	Mail.feaa.uaic	2002:557a:16	Mail
2012/01/22 0	RECEIVE	STOREDRIV		<0A07D5FF3	Catalog Retel	valy.greavu@	adrian.munte	3122775	2002:557a:16	Mail.feaa.uaic	2002:557a:16	Mail
2012/01/22 1	RECEIVE	STOREDRIV		<0A07D5FF3	RE: Catalog	valy.greavu@	adrian.munte	3123075	2002:557a:16	Mail.feaa.uaic	2002:557a:16	Mail
2012/01/22 2	RECEIVE	STOREDRIV		<0A07D5FF3	Anton Andree	valy.greavu@	adrian.munte	3123283	2002:557a:16	Mail.feaa.uaic	2002:557a:16	Mail
2012/01/23 1	RECEIVE	STOREDRIV		<0A07D5FF3	RE: Dosare g	valy.greavu@	fdumi@uaic.r	3123768	2002:557a:16	Mail.feaa.uaic	2002:557a:16	Mail
2012/02/03 1	RECEIVE	STOREDRIV		<0A07D5FF3	RE: Criterii d	valy.greavu@	fdumi@uaic.r	3140435	2002:557a:16	Mail.feaa.uaic	2002:557a:16	Mail
2012/02/07 1	RECEIVE	STOREDRIV		<0A07D5FF3	RE: Criterii d	valy.greavu@	fdumi@uaic.r	3154025	2002:557a:16	Mail.feaa.uaic	2002:557a:16	Mail
2012/02/09 1	RECEIVE	STOREDRIV		<0A07D5FF3	Read: Sold	valy.greavu@	adrian.munte	3156588	2002:557a:16	Mail.feaa.uaic	2002:557a:16	Mail

Figura nr. 8.5 – *Lista detaliată de mesaje între doi utilizatori (Exchange Server)*

Detalii despre primul mesaj.

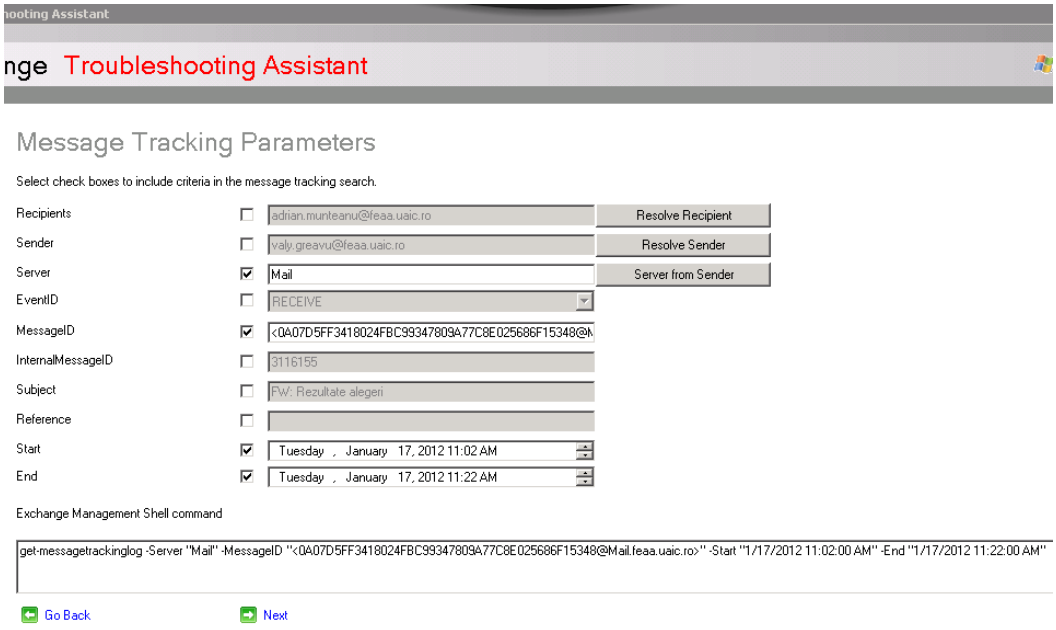


Figura nr. 8.6 – *Afişarea detaliilor despre un anumit mesaj*

Rezultatul este schimbul complet de mesaje pe subiectul specificat in MessageID.

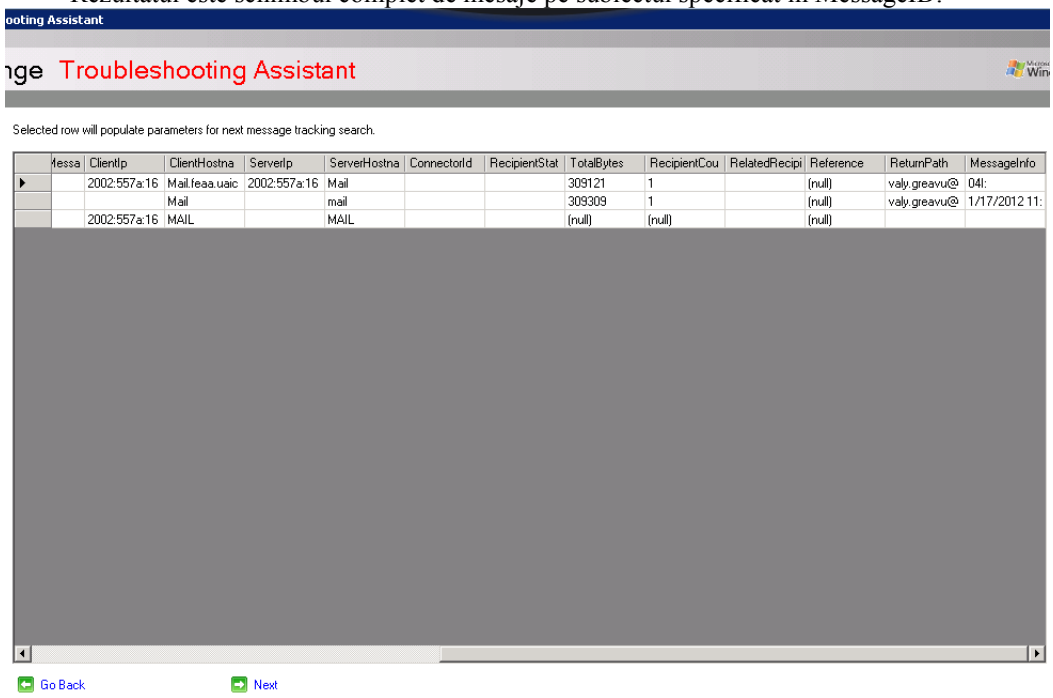

Troubleshooting Assistant
Selected row will populate parameters for next message tracking search.
Xessa | ClientIp | ClientHostna | ServerIp | ServerHostna | ConnectorId | RecipientStat | TotalBytes | RecipientCou | RelatedRecipi | Reference | ReturnPath | MessageInfo
2002:557a:16 | Mail.feaa.uaic | 2002:557a:16 | Mail | 309121 | 1 | (null) | valy.greavu@ | 04l:
Mail | mail | 309309 | 1 | (null) | valy.greavu@ | 1/17/2012 11:
2002:557a:16 | MAIL | MAIL | (null) | (null) | (null)
Go Back
Next

Figura nr. 8.7 – *Schimbul complet de mesaje între doi utilizatori pe un anumit subiect*

Capitolul 9. Dispozitive de stocare amovibile

S-a întâmplat de multe ori să fim nevoiți să analizăm cine a lucrat cu un stick de memorie USB şi dacă a copiat un fişier cu informații confidențiale ale organizației. Ori de cîte ori un astfel de dispozitiv este ataşat unui sistem pe care rulează Windows rămân „amprente" în Regitry.

9.1 Dispozitive USB şi Registry

Ori de câte ori un dispozitiv amovibil de tipul memoriilor portabile este ataşat unui sistem Windows, Plug and Play Manager (PnP) identifică un astfel de eveniment şi interoghează descriptorul dispozitivului cu privire la informații despre producător[48]. PnP Manager va folosi aceste informații pentru a identifica ulterior driver-ul necesar funcționării dispozitivului. Odată identificat dispozitivul, în Registry va fi creată o subcheie:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\enum\USBSTOR
```

În această subcheie se identifică subcheile de tipul:

```
Disk&Ven_###&Prod_###&Rev_###
```

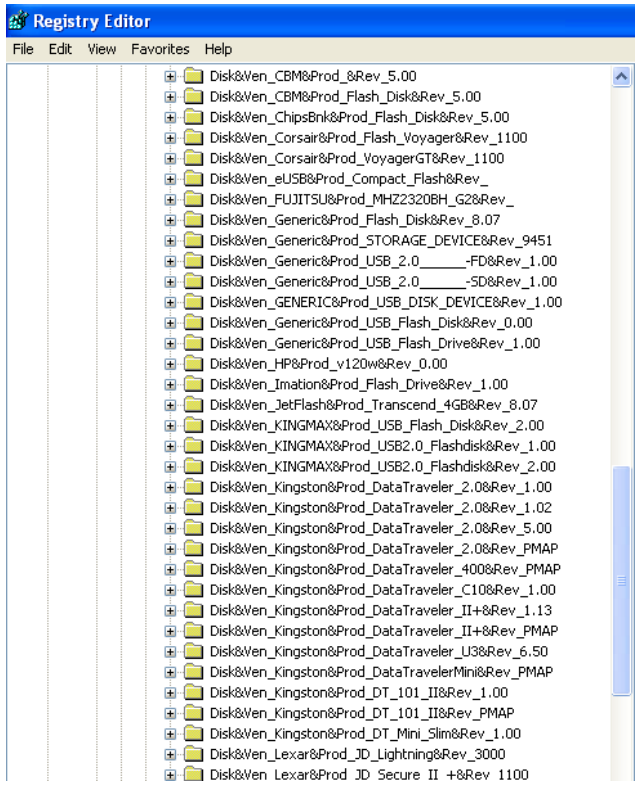


Figura nr. 9.1 – *Istoricul dispozitivelor amovibile care au fost introduse într-un sistem de calcul*

[48] Aceste informații nu sunt disponibile în zona disponibilă pentru stocarea informațiilor ci în ceea ce se numeşte „firmware".

Cheia reprezintă identificatorul clasei din care face parte dispozitivul. Nu toate dispozitivele amovibile au asociat un număr serial. În cazul în care au, acest număr identifică în mod unic fiecare instanță a aceluiaș dispozitiv.[49]

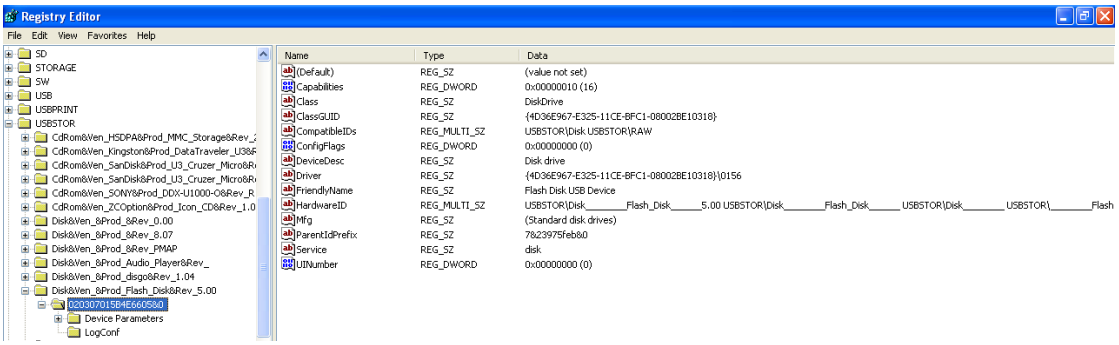


Figura nr. 9.2 – *Detalii despre un anumit dispozitiv amovibil*

Pentru dispozitivele pentru care nu poate fi identificat numărul serial, PnP Manager va crea o instanță unică identificată astfel:

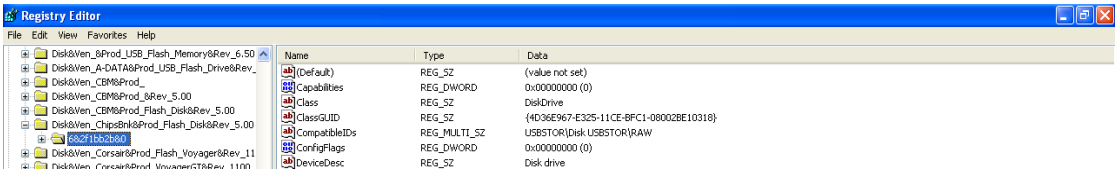


Figura nr. 9.3 – *Alte detalii despe istoricul dispozitivelor amovibile*

Altfel spus dacă o instanță din această subchei din Registry nu conține caracterul „&” putem identifica în mod unic dispozitivul care a fost atașat la un moment dat calculatorului investigat. Problemele se complică când, așa după cum se observă din imaginile anterioare, pe un calculator au fost utilizate mai multe astfel de dispozitive. În acest caz avem nevoie de un utilitar[50] care să ne permită să navigăm mai ușor printre cheile Registry, centralizat.

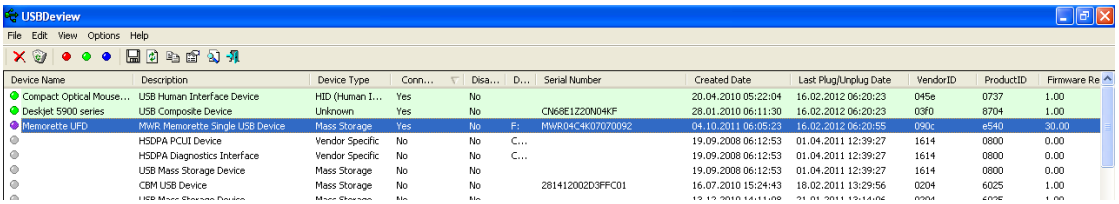


Figura nr. 9.4 – *Utilitarul USBDeview*

[49] Cazul în care calculatorului i-au fost atașate două dispozitive de același tip, de la același producător.

[50] UVCView. Acest utilitar este integrat acum în Windows Driver Kit (WDK) disponibil pentru Windows 7 la adresa http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11800 . Pentru versiuni anterioare Windows 7, utilitarul este disponibil pentru descărcare pe diferite forumuri/situri ce tratează subiectul „forensic”. Se poate folosi si USBDeview v2.00

Utilitarul de mai sus ne oferă informaţii cu privire la data şi ora la care a fost ataşat prima dată şi ultima dată un anumit dispozitiv de stocare. Nu ştim însă dacă s-a şi scris ceva pe el.

Informaţii despre dispozitivele instalate pe un sistem pe care rulează o versiune a sistemului de operare Windows vom găsi şi în fişierul *setupapi.log*. În imaginea de mai sus observăm că un memory stick cu numele Memorette a fost instalat în data de 04.10.2011 , ora 06:05:23. Dacă verificăm fişierul *setupapi.log* ar trebui să regăsim aceeaşi informaţie:

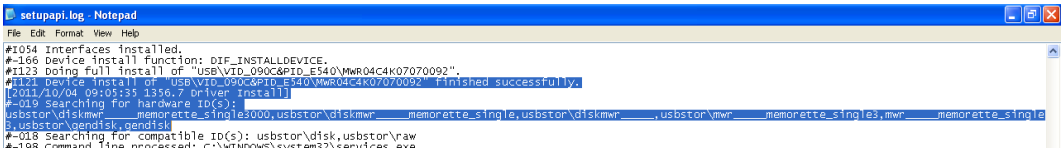

setupapi.log - Notepad
File Edit Format View Help
#I054 Interfaces installed.
#-166 Device install function: DIF_INSTALLDEVICE.
#I123 Doing full install of "USB\VID_090C&PID_E540\MWR04C4K07070092".
#I121 Device install of "USB\VID_090C&PID_E540\MWR04C4K07070092" finished successfully.
[2011/10/04 09:05:35 1356.7 Driver Install]
#-019 Searching for hardware ID(s):
usbstor\diskmwr_____memorette_single3000,usbstor\diskmwr_____memorette_single,usbstor\diskmwr_____,usbstor\mwr_____memorette_single3,mwr_____memorette_single
3,usbstor\gendisk,gendisk
#-018 Searching for compatible ID(s): usbstor\disk,usbstor\raw

Figura nr. 9.5 – *Fişierul jurnal setupapi.log*

Diferenţa de timp rezultă din modul în care se raportează la sistemul temporar utilitarul USBDeview.

9.2 Dispozitive portabile şi Registry

O cheie din Registry ce merită atenţie este:

`HKEY_LOCAL_MACHINE\Sostware\Microsoft\Windows Portable Decives\Devices`

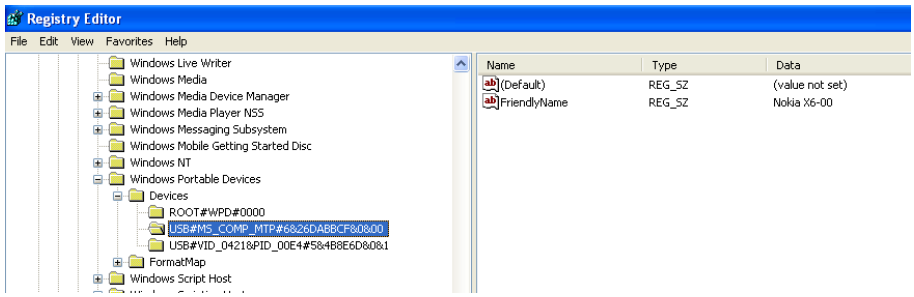


Figura nr. 9.6 – *Cheia de registry FriendlyName*

În subcheile acestei chei vom găsi valoarea *FriendlyName* care este identică cu ceea ce afişează My Computer în momentul în care se ataşează calculatorului un dispozitiv portabil.

Utilitarul USBDeview ne oferă însă mai multe informaţii:

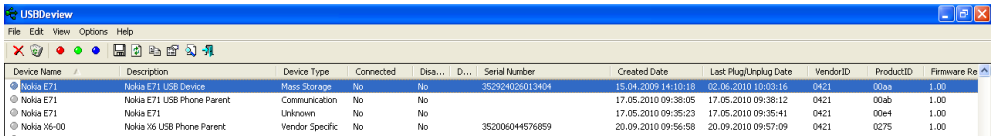


Figura nr. 9.7 – *Detalii despre dispozitivele amovibile în USBDeview*

Din imaginea de mai sus observăm că a fost vorba de două telefoane mobile de la producătorul Nokia, modele E71 respectiv X6. Utilitarul afişează şi numărul serial al dispozitivului ataşat, aceasta fiind o informaţie foarte importantă.

În cazul în care dorim să verificăm dacă un fişier conţinând informaţii critice a fost copiat în mod neautorizat, lucrurile se complică foarte mult. Dacă am avea la dispoziţie ambii suporţi de memorare (cel sursă, de pe care s-a copiat, respectiv cel destinaţi, pe care s-a copiat) am putea analiza informaţiile despre cele două fişiere. Din acest motiv nu se va putea spune cu certitudine dacă fişierul a fost copiat de pe un anumit mediu de stocare. Putem însă obţine informaţii dacă un fişier a fost copiat pe un anumit mediu de stocare!

Să luăm ca exemplu starea fişierului *Auditat.doc*, înainte şi după copierea pe un stick de memorie :

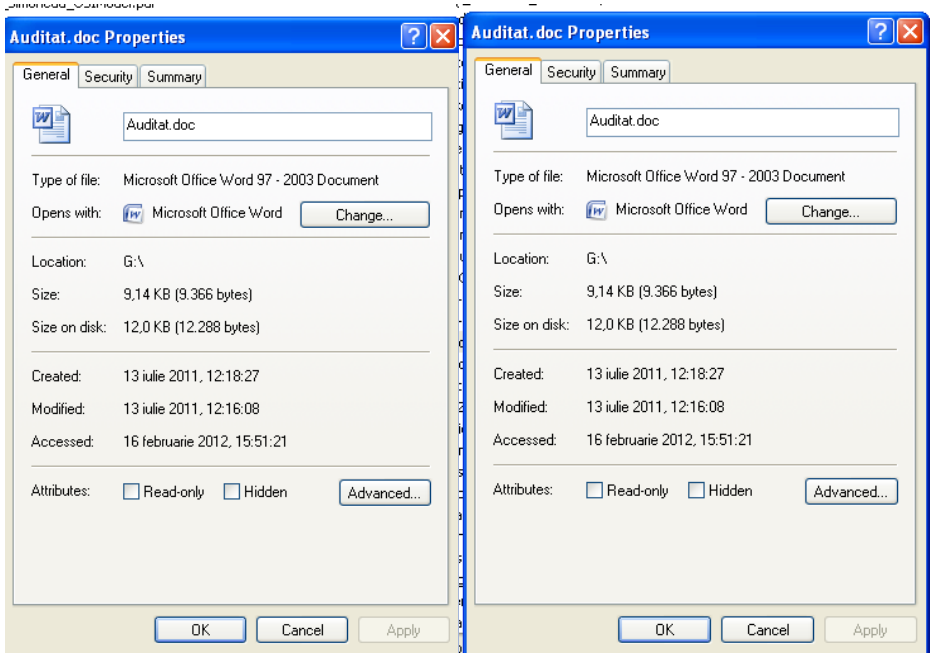


Figura nr. 9.8 – *Proprietăţile unui fişier înainte de copierea pe un dispozitiv extern*

Se observă că proprietăţile fişierului nu sunt modificate. Pe suportul destinaţie – stickul de memorie, situaţia se prezintă astfel:

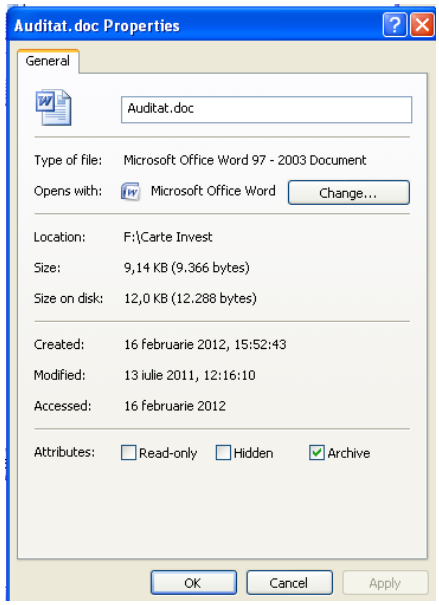
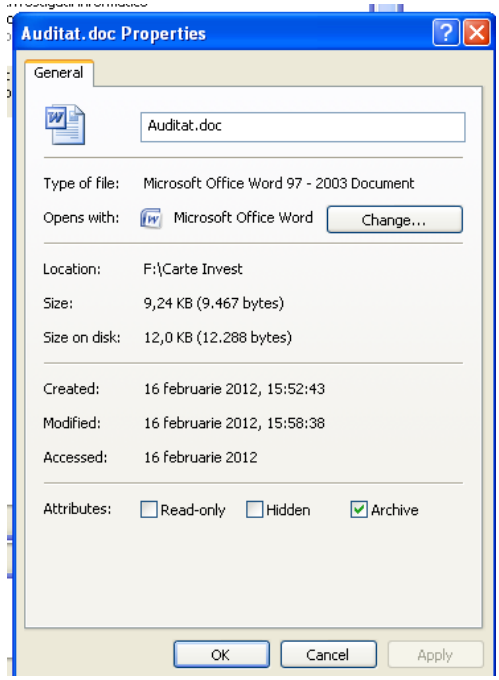


Figura nr. 9.9 – *Proprietățile unui fişier după copierea pe dispozitive externe*

Am putea spune că avem probe. Situația nu este chiar aşa. Dacă fişierul copiat în mod neautorizat a fost deschis şi s-a modificat ceva în el, informațiile disponibile se modifică şi ele:



În acest exemplu nu am luat în calcul opțiunea Auto Save care este de obicei activă în cazul editorului de texte MS Word. Despre metadate vom discuta ulterior.

Capitolul 10. Virtualizare şi instrumente specifice investigaţiilor

După cum sugerează şi titlul, în cele ce urmează vor fi puse în discuţie aspectele ce privesc maşinile virtuale. Mai exact sunt descrise atât aspectele teoretice ale unei maşini virtuale dar şi cele practice şi anume: instalarea unei maşini virtuale, cu paşii corespunzători, configurarea acesteia dar şi utilităţile unei astfel de maşini.

10.1 Maşinile virtuale – aspecte teoretice

O *maşină virtuală* este o aplicaţie capabilă să interpreteze anumite instrucţiuni care rulează pe o maşină fizică. Aceasta face posibilă rularea unui alt sistem de operare într-o "fereastra" a sistemului de operare principal, fără a repartiţiona hard-disk-ul. De exemplu se poate rula un Windows Xp într-o fereastră a Windows7. Sau se poate rula Linux într-o fereastră a Windows, şi invers. Este ca şi cum ai avea un alt calculator (virtual) pe care îl poţi porni/opri ca pe un program obişnuit.

Suportul pentru maşini virtuale se instalează ca un program obişnuit (exemplu : Vmware, Virtualbox, Virtual PC, etc). După instalare, câteva configurări stabilesc cât din sistemul real poate împrumuta maşina virtuală (memorie, disk). Maşina virtuală are un bios virtual, unde poţi alege de unde să booteze, etc. După pornirea maşinii virtuale se poate boota de pe CD/DVD şi instala sistemul de operare dorit. Pot exista mai multe maşini virtuale create şi chiar rulând în acelaşi timp. Maşinile virtuale se pot apoi şterge de pe hard-disk ca un director obişnuit cu fişiere. Maşinile virtuale funcţionează ceva mai încet decât un sistem de operare instalat direct pe hard disk – diferenţa este mai mică la procesoare mai noi care suportă hardware virtualizare. Totuşi nu se simte o diferenţă notabilă la utilizări obişnuite (Internet, Office, Muzică).

Programele rulate în maşina virtuală nu sunt interpretate "instrucţiune cu instrucţiune". Instrucţiunile rulează nativ pe procesor, doar apelurile care merg spre sistemul fizic sunt înlocuite cu apeluri gestionate de maşina virtuală. Astfel programele care nu lucrează mult cu sistemele periferice (disk, video, audio, reţea) pot rula aproape la aceeaşi viteză ca un sistem instalat nativ. Maşinile virtuale pot boota şi alte partiţii fizice ale disk-ului real, dar este destul de periculos.

10.1.1. Instalarea unei maşini virtuale

Pentru exemplificarea instalării unei maşini virtuale am ales aplicaţia VirtualPC, un produs al companiei Microsoft lansat în 2004. La baza acestui produs stă motorul de maşină virtuală realizat de

compania *Conectix*. Acest produs este o maşină virtuală cu ajutorul căreia se pot crea calculatoare virtuale pe care se pot instala sisteme de operare. Aplicația a fost realizată în două variante: *workstation* (stație de lucru) şi *server*.

Aplicația pune la dispoziția maşinii virtuale pe care o creează toate componentele care pot fi găsite pe un calculator şi, în afară de procesor, toate sunt virtuale. Pentru a funcționa, un calculator are nevoie de placa de bază, procesor, memorie internă şi memorie externă, placă video, monitor, tastatură, mouse şi, eventual, o placă de rețea pentru conectarea la alte calculatoare, o placă de sunet şi/sau orice alt dispozitiv care este instalat pe sistemul de operare gazdă pentru care aplicația oferă suport virtual.

Aplicațiile pentru maşini virtuale, în general, pun la dispoziția calculatoarelor virtuale un sistem virtual de intrare/ieşire astfel că:[51]

- placa video pentru acestea este virtuală, iar monitorul este constituit dintr-o zonă din fereastra aplicației;
- în momentul în care zona de afişaj a conținutului din memoria video a calculatorului virtual devine activă, comenzile transmise de mouse şi tastatură vor fi transmise acestuia; desigur că nu toate combinațiile de taste vor fi active, deoarece unele combinații de taste sunt folosite de sistemul de operare gazdă pentru a executa anumite operații, iar altele sunt folosite cu scopul de a reda controlul asupra tastaturii şi mouse-ului sistemului de operare gazdă;
- memoria internă pentru calculatoarele virtuale este constituită de o zonă din memoria internă a calculatorului gazdă şi, pentru ca totul să meargă bine, dimensiunea acesteia nu poate să fie decât un anumit procent din memoria calculatorului gazdă;
- memoria externă, după cum bine se ştie, este constituită în principal din hard-disk, CD-uri şi dischete; hard-disk-urile pentru calculatoarele virtuale sunt constituite, în principal, de fişiere care se află pe calculatorul gazdă; aceste fişiere nu au, după cum ar fi normal, dimensiunea pe care o raportează sistemul de operare de pe calculatorul virtual, ci acestea sunt redimensionate dinamic în funcție de cerințele şi necesitățile sistemului virtual;

[51] Soroiu, C., *Virtual PC 2004 vs.VMWARE 4,* p. 37, *www.ginfo.ro/revista/13_8/tehno.pdf, accesat: 01.12.2011.*

- placa de rețea pentru sistemul de operare virtual este în întregime virtuală şi există mai multe moduri în care se realizează conectarea la rețeaua la care este conectat calculatorul gazdă:
    - se poate întâmpla să nu se dorească conectarea la întreaga rețea prin intermediul plăcii de rețea virtuală, ci doar la sistemul gazdă, astfel maşinile virtuale mai instalează o placă de rețea virtuală pe sistemul gazdă pentru a realiza această conexiune, deşi, pentru comunicare există alte soluții mai bune;
    - calculatorul virtual poate fi mascat în spatele celui gazdă prin utilizarea unor tabele de translație, deci se va identifica pe rețea ca fiind cel gazdă;
    - calculatorul virtual va utiliza una din plăcile de rețea a celui gazdă, având adresă diferită de acesta, pentru a intra în legătură cu celelalte calculatoare din rețea. În cazul în care pe calculatorul gazdă există doar o placă de rețea, aceasta va fi partajată între cele două sisteme, în acest sens existând mai multe tehnici.

Un calculator virtual foloseşte o unitate de dischetă virtuală care poate fi conectată la unitatea de dischetă a sistemului gazdă sau poate fi legată de o imagine a unei dischete (fişier care conține datele stocate în toate sectoarele unei dischete) aflată pe calculatorul gazdă. La fel ca unitatea de dischetă, unitățile CD-ROM sunt virtuale şi pot fi conectate la unitățile de CD-uri ale sistemului gazdă sau la fişiere care conțin imagini de CD-uri având formatul ISO.

10.1.2. Utilitatea maşinilor virtuale[52]

Şi totuşi la ce folosesc maşinile virtuale? O întrebare care este relativ firesc să apară după prezentarea noțiunilor din paragrafele anterioare. Principalele utilități ale unei maşini virtuale sunt prezentate aşadar în cele ce urmează.

1. Posibilitatea de a rula sisteme de operare diferite pe acelaşi calculator fizic fără o reinstalare a acestuia.
    - Odată instalat un sistem de operare (Windows, Linux), care are driverele necesare, se poate instala un program de virtualizare, se pot defini în el una sau mai multe maşini virtuale iar în fiecare maşină virtuală se poate instala câte un sistem de operare. Maşinile virtuale vor avea discuri virtuale, care vor fi stocate ca fişiere pe disk-ul sistemului de operare principal, numit host (gazda). Sistemul de operare instalat în maşina virtuală va avea impresia că are la dispoziție un hard disk real.
    - Maşinile virtuale consumă ceva spațiu pe disk, dar consumă memorie şi procesor doar dacă sunt pornite. Maşinile virtuale "țin minte" modificările

[52] http://mihvoi.blogspot.com/2010/01/utilizare-masini-virtuale-vmware.html, accesat: 01.12.2011.

între două porniri, este ca şi cum ai reporni un calculator real. Când nu mai este necesară maşina virtuală, spaţiul pe disk se poate elibera uşor ştergând fişierele în care maşina virtuală îşi ţine discurile virtuale.

2. Backup foarte uşor.
    - Datorită faptului că maşinile virtuale sunt stocate în fişiere, backup-ul se face pur şi simplu copiind directorul maşinii virtuale în altă parte. Copierea se face cu maşina virtuală oprită.
    - Majoritatea maşinilor virtuale suportă "snapshot-uri", în care se stochează starea instantanee a maşinii virtuale care rulează. Peste un timp, dacă se doreşte acest lucru, maşina virtuală se poate întoarce la acea stare. Acest sistem consumă mai puţin spaţiu decât copierea întregii maşini virtuale (se memorează doar diferenţele).
    - În cazul în care calculatorul s-a defectat sau a fost cumpărat unul mai puternic, un back-up al maşinii virtuale se poate utiliza pe alt calculator.
    - Maşina virtuală se poate opri cu programele deschise, iar la re-pornire va porni exact din starea în care a fost oprită (cu toate programele deschise).
    - O firmă poate crea o maşină virtuală cu tot ce este necesar unui angajat (programe specifice, conexiuni VPN multiple) şi să o distribuie tuturor celor care au nevoie. Oricine are o problema ... re-copiaza maşina virtuală.
3. Posibilitatea de a muta maşina virtuală de pe un calculator pe altul.
    - De exemplu o persoană poate avea acelaşi sistem de operare şi acasă şi la serviciu. Se poate instala acel sistem de operare pe un stick USB sau pe un hard-disk USB. Singura cerinţă este să existe în ambele părţi instalat acelaşi program de virtualizare. Atenţie, maşinile virtuale pe USB funcţionează destul de încet, se recomandă copierea pe hard disk-ul local.
4. Posibilitatea de a testa unele programe cu risc de a fi virusate.
    - Maşinile virtuale au avantajul că ceea ce rulează în interior nu poate afecta sistemul gazdă, în afară de dimensiunea fişierului. Un program virusat care este rulat în maşina virtuală nu poate virusa sistemul gazdă. Dacă apar suspiciuni că s-a instalat un virus, maşina virtuală se poate întoarce la o stare salvată anterior.

10.2. Principalele instrumente Windows Sysinternals

Unele dintre cele mai utilizate şi accesibile instrumente în domeniul investigaţiilor sunt cele de la Sysinternals, companie achiziţionată de către Microsoft.

În continuare vom prezenta o descriere sumară a celor mai reprezentative instrumente şi utilitatea lor specifică.

Denumire	Descriere
AccessChk v2.0	Afişează drepturile de acces la fişiere, cheile Registry sau serviciile Windows, în funcţie de utilizator sau grupuri de utilizatori.
AccessEnum v1.3	Afişează cine a avut acces la un director, fişiere, chei Registry. Este folosit pentru a identifica atribuirea incorectă a permisiunilor.
Autoruns v8.53	Afişează lista aplicaţiilor configurate să pornească automat în momentul în care este pornit sistemul de calcul şi un utilizator efectuează procesul de logon. De asemenea, afişează lista completă a cheilor de regiştri şi locaţiile fişierelor folosite pentru pornirea automată a sistemului de calcul.
Autorunsc v8.53	Utilitarul în formatul linie de comandă folosit pentru identificarea aplicaţiilor configurate să pornească automat la logon.
Diskmon	Realizează o captură (monitorizare şi jurnalizare) a activităţii discurilor.
DiskView	Utilitar în mod grafic pentru vizualizarea structurii şi sectoarelor hardiscurilor.
Du v1.3	Afişează spaţiul utilizat pe disc în funcţie de dimensiunea directoarelor. Este util pentru identificarea directoarelor cu multe informaţii stocate.
Filemon v7.03	Afişează activitatea fişierelor sistem în timp real.
Handle v3.2	Afişează fişierele deschise şi procesele care au deschis şi utilizează aceste fişiere.
ListDLLs v2.25	Afişează toate librăriile DLL care sunt încărcate de aplicaţiile curente, incluzând informaţii despre locaţia de unde au fost încărcate (calea pe disc) şi versiunea fiecărui modul încărcat.
LogonSessions v1.1	Afişează lista sesiunilor de logon active.
PendMoves v1.1	Afişează lista fişierelor care vor fi redenumite sau şterse la următoare repornire a calculatorului. Din cauză că sunt încărcate sau în curs de utilizare anumite fişiere sistem nu pot fi redenumite sau şterse în timpul rulării, de aceea operaţiunile respective sunt reprogramate pentru etapa după repornirea calculatorului.
Portmon v3.02	Afişează activitatea pe porturile seriale şi paralele incluzând pachete de date transmise sau primite pe porturile respective.
Process Explorer v10.2	Afişează o listă de fişiere, chei de regiştri şi alte obiecte deschise de procesele active precum şi lista librăriilor DLL deschise de fiecare proces în parte.

Denumire	Descriere
PsExec v1.72	Permite posibilitatea de executare a anumitor comenzi de la distanță, folosind privilegiile potrivite.
PsFile v1.01	Afișează o listă a fișierelor deschise.
PsInfo v1.71	Afișează informații despre un anumit calculator.
PsList**Error! Bookmark not defined.** v1.27	Afișează informații despre procese și firele de execuție.
PsLoggedOn v1.32	Afișează numele utilizatorului conectat pe un calculator.
PsLogList v2.63	Realizează un export a înregistrărilor din Event log.
PsService v2.2	Permite vizualizarea și controlul serviciilor Windows.
Regmon v7.03	Afișează în timp real activitatea regiștrilor Windows.
RootkitRevealer	Realizează o scanare a discului în vederea descoperirii aplicațiilor de tip Rootkit.
ShareEnum v1.6	Scanează toate resursele partajate în rețea pentru a vizualiza setările de securitate în scopul eliminării configurărilor improprii.
Strings v2.3	Permite căutarea după text ascuns în fișierele de tip imagine. Este o măsură de identificare a steganografiei.

10.3 Principalele instrumente native Windows

Name	Description
Arp	Afișează tabela ARP (Address Resolution Protocol)
Date	Afișează data și ora curentă a sistemului
Dir	Afișează o listă a directoarelor și subdirectoarelor de pe un disc.
Doskey	Afișează un istoric al comenzilor executate într-o consolă deschisă de cmd.exe.
Ipconfig	Afișează configurația TCP/IP a calculatorului curent.
Net	Actualizare, configurare sau afișare a dispozitivelor de rețea sau legate de accesul la rețea Net este doar rădăcina unui set de comenzi destinate configurării/afișării setărilor despre sesiunile active, fișierele deschise, utilizatori, resurse partajate etc.
Netstat	Afișează statistici despre conexiunile în rețea.

Name	Description
Time	Afişează ora curentă a sistemului.
Find	Se foloseşte pentru căutarea fişierelor pe disc.
Schtasks	Afişează acţiunile programate să se execute la anumite perioade de timp.
Systeminfo	Oferă informaţii cu caracter general despre sistemul de calcul curent.
Vol	Afişează eticheta unui disc şi numărul unic de identificare, daca acestea există.
Hostname	Afişează numele complet al calculatorului.
Openfiles	Afişează o listă cu fişierele deschise de pe calculatorul curent de alţi utilizatori din reţea.
FCIV	File Checksum Integrity Verifier – Se foloseşte pentru a verifica suma de control a unui fişier pe baza metodelor criptografice MD5 sau SHA1.
Notepad	Se foloseşte în principal ca editor simplu de text, dar se poate folosi cu scopul de a vizualiza metadatele asociate unui fişier de orice tip.
Reg	Este un utilitar de tip linie de comandă pentru afişarea, modificarea, exportul, salvarea sau ştergerea unor chei sau valori din regiştri.
Netcap	Se foloseşte pentru a prelua informaţii despre traficul de reţea în formatul linie de comandă.
Sc	Se foloseşte pentru afişarea detaliată a stării serviciilor Windows în format linie de comandă dar şi pentru pornirea sau oprirea serviciilor Windows reprezentând un instrument mai elaborat decât net start.
Assoc	Vizualizarea şi modificarea asocierilor dintre extensiile fişierelor şi aplicaţiile cu care acestea se pot deschide.
Ftype	Se foloseşte pentru afişarea sau modificarea asocierilor dintre tipurile de fişiere şi aplicaţiile cu care acestea se pot deschide.
Gpresult	Se foloseşte pentru evaluarea aplicării unei politici de securitate specifice pentru un anumit utilizator determinat.
Tasklist	Afişează lista proceselor active precum şi a modulelor încărcate.
MBSA	Utilitar specific determinării nivelului de securitate a unui calculator prin evaluarea patch-urilor de securitate aplicate, modul de configurare a serviciilor, aplicaţiilor şi utilizatorilor.
Rsop.msc	Se foloseşte pentru a afişa rezultatul combinării diferitelor politici de securitate provenind din mai multe surse pe calculatorul curent.

Name	Description
Rasdiag	Colectează informaţii despre serviciile de conectare de la distanţă şi stochează aceste date în fişiere jurnal.

10.4. FTK 4.0

Forensic Toolkit® (FTK®) este recunoscut in lumea întreagă ca una din cele mai bune aplicaţii software pentru investigaţii criminaliste digitale. Aceasta platformă de investigare digitala oferă software de analiza criminalistica pe calculator, decriptare si spargere de parole, toate in cadrul unei interfeţe intuitive si personalizabile. Forensic Toolkit 4 este acum cel mai avansat software criminalistic pentru calculatoare, oferind o funcţionalitate pe care in mod normal numai organizaţii cu zeci de mii de dolari si-ar putea-o permite. Totuşi, AccessData si-a făcut tehnologia disponibila tuturor investigatorilor si analiştilor, indiferent daca sunt in educaţie, agenţii guvernamentale, corporaţii din cadrul Fortune 500, sau realizează investigaţii digitale ca furnizor de servicii criminalistice pentru calculatoare.

Nu avem pretenţia că paginile ce urmează reprezintă un manual de utilizare în sensul larg al înţelesului. Suita FTK este suficient de complexă. Prin urmare vom prezenta doar lucrurile esenţiale, urmând ca cititorul să descopere celelalte facilităţi pe măsură ce avansează cu lucrul.

10.4.1. Interfaţa utilizatorului

Nu vom insista cu descrierea etapelor instalării acestei suite de aplicaţii. Lucrurile sunt suficient de clare sau cel puţin intuitive. Pornim la lucru direct cu momentul lansării în execuţie a FTK.

1. Din fereastra *Case Manager*, click *Case > New*.
2. Se pot specifica opţiuni cu privire la probe prin click *Detailed Options* din fereastra *New Case Options*.
3. Se bifează opţiunea *Open the Case*, şi apoi click *OK*.

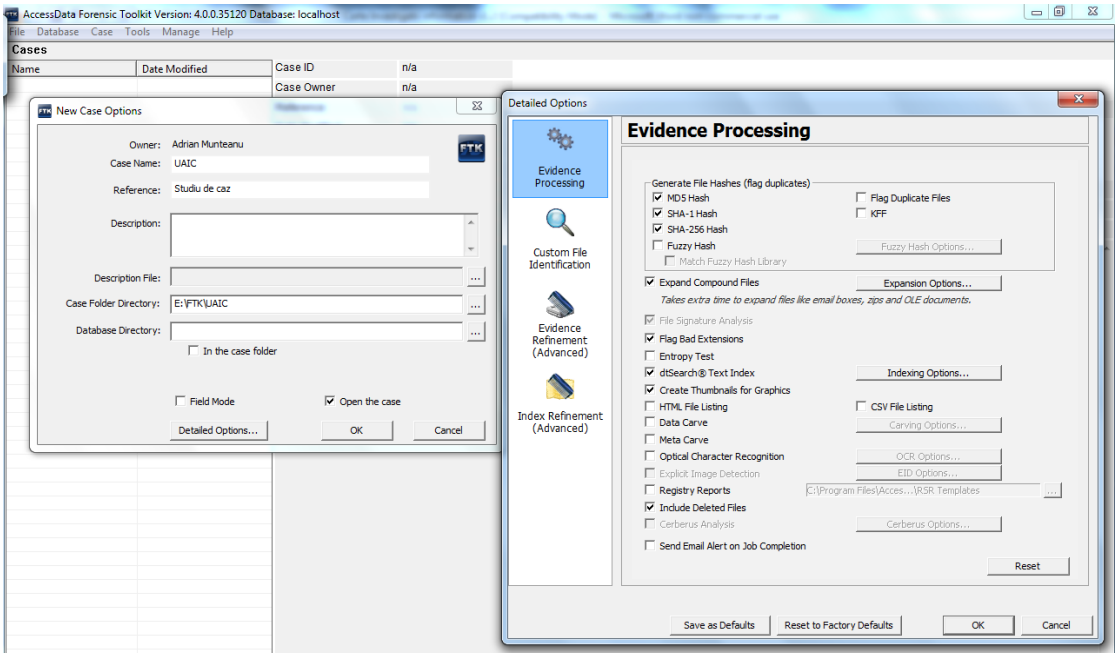
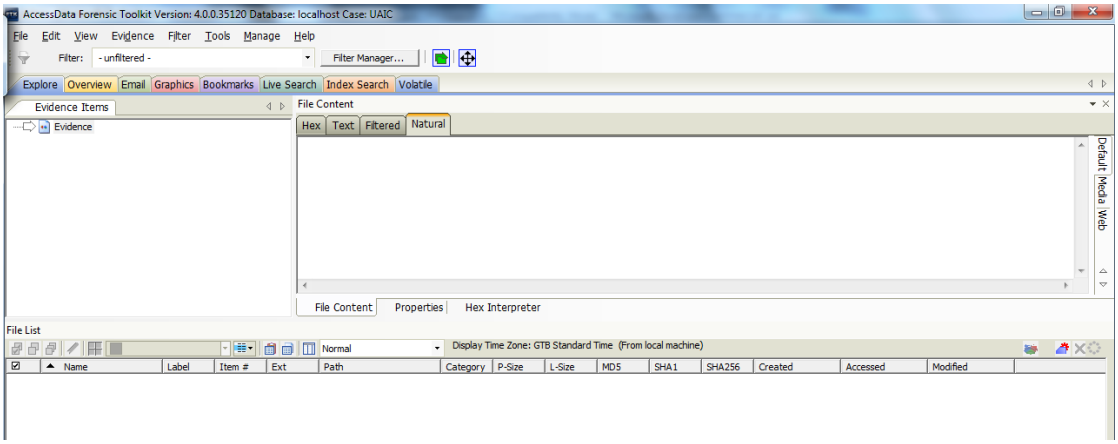
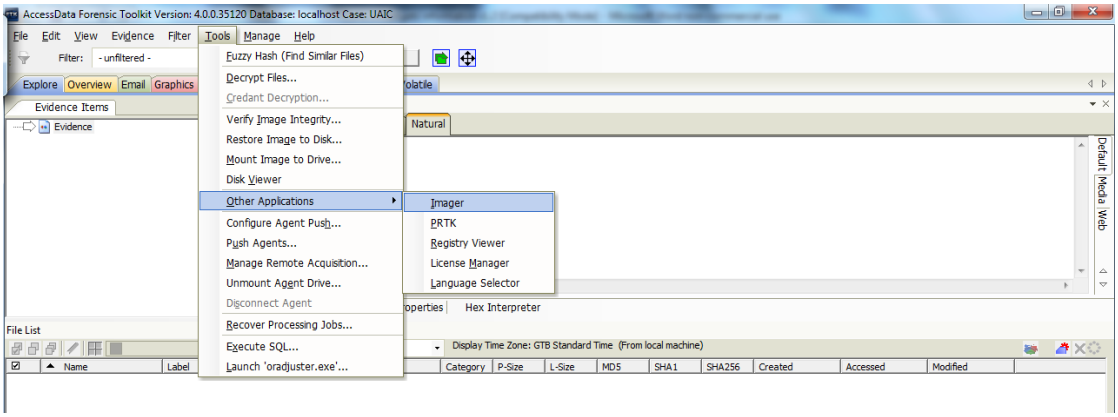


Figura nr. 10.1 – *Procesarea evidențelor electronice în FTK*

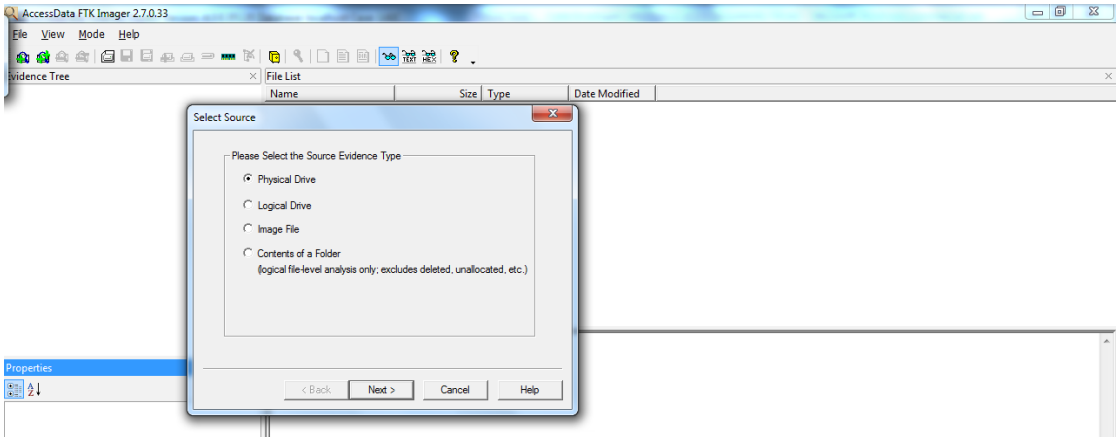
4. Se așteaptă crearea cazului. La finalul acestui proces FTK va deschide o nouă fereastră


AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: UAIC
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
Evidence Items
Evidence
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List
Normal
Display Time Zone: GTB Standard Time (From local machine)
Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created Accessed Modified

În situația în care proba încă nu a fost colectată, va trebui să facem apel la FTK Imager:



După alegerea acestei opțiuni se deschide fereastra specifică aplicației lansată în execuție, de unde va trebui să alegem tipul de probă pe care dorim să o realizăm:



Pentru că spațiul nu ne permite şi nu am pornit să scriem un manual de utilizare (Manualul de utilizare FTK numără 392 de pagini) vom presupune că am colectat deja probele pe un memory stick.

Capitolul 11. Raportul de expertiză

11.1 Reglementări

Ordonanța Guvernului nr. 2/2000 privind organizarea activității de expertiză tehnică judiciară şi extrajudiciară, cu modificările şi completările ulterioare (Legea nr. 37/2009, Legea nr. 178/2009, Ordonanța Guvernului nr. 13/2010, Legea nr. 208/2010), Ordinul nr. 1322/C din 21 iunie 2000 pentru aprobarea Regulamentului privind atribuirea calității de expert tehnic judiciar şi de specialist precum şi Ordinul Nr. 199/C din 18 ianuarie 2010 pentru aprobarea Nomenclatorului specializărilor expertizei tehnice judiciare, sunt actele juridice ce reglementează domeniul expertizelor judiciare

Din OG 2/2000 ştim că:

„ART. 1

(2) Este expert tehnic judiciar orice persoană fizică ce dobândeşte această calitate în condițiile prezentei ordonanțe şi este înscrisă în tabelul nominal cuprinzând experții tehnici judiciari, întocmit, pe specialități şi pe județe, respectiv pe municipiul Bucureşti. Expertul tehnic judiciar este expert oficial şi poate fi numit de organele de urmărire penală, de instanțele judecătoreşti sau de alte organe cu atribuții jurisdicționale pentru efectuarea de expertize tehnice judiciare.

ART. 2

Expertiza tehnică efectuată din dispoziția organelor de urmărire penală, a instanțelor judecătoreşti sau a altor organe cu atribuții jurisdicționale, de către expertul sau specialistul numit de acestea, în vederea lămuririi unor fapte sau împrejurări ale cauzei, constituie expertiză tehnică judiciară"

Aceeaşi Ordonanță stabileşte şi *regulile procedurale privind expertiza tehnică judiciară:*

„ ART. 21

Raportul de expertiză cuprinde:

a) partea introductivă, în care se menționează organul care a dispus efectuarea expertizei, data la care s-a dispus depunerea acesteia, numele şi prenumele expertului sau ale experților, specialitatea acestuia/acestora, data întocmirii şi finalizării raportului de expertiză, obiectul acesteia şi întrebările la care expertul sau experții urmează să răspundă, bibliografia pe baza căreia expertiza a fost efectuată şi dacă părțile care au participat la aceasta au dat explicații în cursul lucrărilor la care au fost convocate;

b) descrierea operațiunilor de efectuare a expertizei, obiecțiile sau explicațiile părților, precum şi analiza acestor obiecții ori explicații pe baza celor constatate de expert sau de specialist;

c) concluziile, care cuprind răspunsurile la întrebările puse şi părerea expertului sau a specialistului asupra obiectului expertizei."

Trebuie cunoscute şi prevederile Codului de procedură civilă, cu modificările şi completările ulterioare: art. 1081 – 1085 (Amenzi judiciare şi despăgubiri), art. 130, art. 170, art.

1711, art. 201 – 214 (Expertiza), Codul de procedură penală, cu modificările şi completările ulterioare: art. 116 – 127 (Secţiunea X – Expertizele), art. 198 – art. 199 (Abateri judiciare).

11.2 Conţinutul raportului de expertiză – ghid

După cum se vede şi din reglementarea citată anterior, raportul de expertiză pare a nu avea o structură prea complexă sau prea standardizată. În opinia noastră este important însă să dezvoltăm această componentă.

Raportul de expertiză este instrumentul prin care expertul comunică rezultatele muncii sale, rezultat concretizat sub formă de probe. Chiar dacă speţele sunt foarte diferite, există câteva elemente ce ar trebui să se regăsească în orice raport, în baza cerinţelor impuse prin reglementările menţionate. Vom vedea însă că există câteva particularităţi ale acestui raport.

Raportul, chiar dacă va conţine tehnicisme, trebuie să fie uşor de citit. Ideile trebuie exprimate de o manieră logică care să conducă la construirea unei argumentaţii: ideile comune grupate în paragrafe; paragrafele grupate în secţiuni.

Din punct de vedere al stilului, trebuie evitate generalizările şi observaţiile personale. Scopul raportului de expertiză este să demonstreze adevărul nu să acuze sau să apere o persoană! Implicarea emoţională este exclusă, indiferent de cauza pentru care se solicită expertiza.

RAPORT DE EXPERTIZĂ TEHNICĂ JUDICIARĂ

Capitolul I, INTRODUCERE

Subsemnatul Munteanu Adrian expert tehnic judiciar în specialitatea_____, posesor al legitimaţiei de expert tehnic nr. _____ am fost numit în sedinţa din _____ expert tehnic judiciar în dosarul nr. _____ , părţile implicate în proces fiind:
1. _____
2._____
n._____ (Pentru fiecare parte implicată în proces se va menţiona: denumirea, domiciliul sau sediul social şi calitatea procesuală)

Împrejurările şi circumstanţele în care a luat naştere litigiul sunt:
_____
_____

Pentru rezolvarea acestei cauze s-a dispus proba cu expertiza tehnică, căreia i s-au fixat următoarele obiective (întrebări):
1. _____
2. _____ _____
n. _____ _____

Lucrările expertizei tehnice s-au efectuat în perioada _____ la sediul social /domiciliul
_____

Materialul documentar şi tehnic care a stat la baza efectuării expertizei constă în:

_____

Redactarea prezentului raport de expertiză tehnică s-a făcut în perioada _____.

În cauză s-au efectuat /nu s-au efectuat alte expertize tehnice; s-au utilizat /nu s-au utilizat lucrările altor experți (tehnici fiscali etc.).
Problemele ridicate de părțile interesate în expertiză şi explicațiile date de acestea în timpul efectuării expertizei sunt:
_____
_____

Data pentru depunerea prezentului raport de expertiză tehnică a fost fixată la şi prelungită la _____.
(dacă este cazul)

CAPITOLUL II, DESFĂŞURAREA EXPERTIZEI TEHNICE

Obiectivul nr. ...

Pentru a răspunde la obiectivul (întrebarea nr. i) s-au examinat următoarele documente/acte/dispozitive/echipamente: _____ (descriere detaliată dacă este cazul)

În conformitate cu probele expertizate formulăm, la obiectivul nr. I, următorul răspuns:_____ (se redactează răspunsul clar, concis şi fără ambiguități)

CAPITOLUL III, CONCLUZII

În conformitate cu examinările materialului documentar menționat în introducerea şi cuprinsul prezentului raport de expertiză tehnică formulăm următoarele concluzii (răspunsuri) la obiectivele (întrebările) fixate acesteia:

La obiectivul nr. 1 _____
La obiectivul nr. 2 _____
La obiectivul nr. n _____ (Se vor relua răspunsurile din capitolul II, DESFĂŞURAREA EXPERTIZEI TEHNICE)

Pentru ca prezentul raport de expertiză tehnică să vină în sprijinul beneficiarului, considerăm necesar să facem următoarele precizări:
_____
_____
_____.
(Acest paragraf poate fi introdus numai dacă expertul tehnic consideră că este util beneficiarului expertizei tehnice. El poate face obiectul unui capitol separat: CAPITOLUL IV, CONSIDERAȚIILE PERSONALE ALE EXPERTULUI(ȚILOR) TEHNIC(I).)

Față de această situație, instanța de judecată va hotărî.

Expert(ți) Tehnic(i):

Ținând cont de posibila volatilitate a probelor, este recomandabil ca în raportul de expertiză să se menționeze durată fiecărei investigații:

- Data de început a investigației: 10 ianuarie 2012, 8.30
- Data de finalizare a investigației: 12 februarie 2012, 17.45
- Durata investigației: 150 ore
- Sisteme de operare examinate: Microsoft Windows Server 2003 R2, Windows XP SP 3
- Sistemul de fișiere: NTFS
- Cantitatea de informații analizate ("imaginea"): 1,200,000 MB

Descriere probe:

Proba nr. 1: Server tip rack IBM X-Series 360, Serial Number 111-A1111-11-111-1111.

Data	Acțiune
11.01.2012, 10:30	Ridicarea serverului din sala serverelor. Achiziția datelor de pe hard diskurile serverului prin protejarea acestora la scriere. S-a folosit FTK Imager.
12.01.2012, 10:00	Analiza probelor colectate. Au fost identificate fișierele probatorii. S-au documentat activitățile realizate.

Probe:

- Serverul a fost accesat local. Serviciul director Active Directory a fost modificat prin acordarea de privilegii suplimentare de tipul Domain Administrators utilizatorului Valy Greavu. Data realizării acestor modificări este 24.12.2011, ora 21.20. Contul activ în acel moment a fost abcbank\Administrator
- Pentru directorul Y:\ServiciiNoi a fost asignat ca proprietar (owner) Valy Greavu.
- Fișierul Y:\ServiciiNoi\Campanie_produse_corporate.doc a fost accesat prin intermediul contului Valy Greavu în data de 25.12.2011, ora 23.51.
- Fi;ierul Y:\ServiciiNoi\Confidential\StrategieNouă.doc a fost accesat prin

intermediul contului Valy Greavu în data de 25.12.2011, ora 23.57

.

Proba nr. 2: Tablet laptop Fujitsu Siemens7400, Serial Number 222-B2222-22-22-2222.

Date / time	Action
11.01.2012, 10:35	Ridicare laptop aflat în posesia lui Valy Greavu
14.01.2012, 10:00	Analiza probelor colectate. Au fost identificate fişierele şi evenimentele probatorii. S-au documentat activităţile realizate.

Probe:

- Laptopul a fost accesat cu contul abcbank\valy.greavu în data de 24.12.2011, ora 21.18.
- Fişierele Campanie_produse_corporate.doc respectiv StrategieNouă.doc au fost transferate de pe server în directorul local My Documents.
- A fost pornită aplicaţia Internet Explorer şi s-a accesat pagina www.gmail.com în data de . 24.12.2011, ora 23.58.

  Fişierele au fost transmise către adresa gigel.popescu@hotmail.com în data de 25.12.2011, ora 00.03

CONCLUZIE

1. **La obiectivul nr. 1:**

Concluzionăm că Valy Greavu – Corporate Manager a obţinut în mod neautorizat acces la fişiere conţinând informaţii clasificate "Confidenţial" şi le-a transferat prin poştă electronic către o terţă parte.

În final mai menţionăm că un raport asupra datelor investigate se poate obţine cu majoritatea software-urilor de tip forensic. În acest caz trebuie să adaptaţi formatul raportului obţinut în mod automat la cerinţele legiuitorului.

Studii de caz practice

Capitolul 12. Studiul de caz 1 – Sustragere informații

În continuare va fi simulat un caz de investigare electronică.

Cazul pleacă de la ideea că un angajat a unei întreprinderi care realizează diverse produse de alimentație, sustrage rețete clasificate ca fiind secrete în ideea de a le vinde unei întreprinderi concurente.

Vom presupune, pe rând, mai întâi că suntem inculpatul şi vom folosi câteva tehnici de ascundere a dovezilor iar apoi vom intra în rolul unui investigator care analizează stickul pe care am ascuns dovezile.

12.1 Partea I – Ascunderea informațiilor

În partea întâi a aceste lucrări practice presupunem că suntem persona acuzată de furtul informațiilor. Acuzatul este şi vinovat în cazul nostru şi deține pe un stick USB rețete secrete ale întreprinderii în care este angajat.

În continuare misiunea noastră ca inculpat este să ascundem fişierul respectiv.

Este vorba de un fişier Excel în care avem rețete secrete de fabricație. Cunoaştem riscurile la care ne supunem, am documentat bine problema şi ştim ce avem de făcut pentru a ascunde fişierul astfel încât să fie aproape imposibil de găsit în cazul în care suntem descoperiți.

Pasul 1 Denumirea şi protejarea documentului cu parolă

În multe cazuri, un angajat care sustrage documente secrete se limitează la redenumirea fişierului în speranța că un investigator va căuta explicit documente care descriu în denumire conținutul, de exemplu retete_secrete.xlsx. Noi presupunem că deținem cunoştințe mult mai avansate de atât şi pe lângă denumirea fişierului în lista_cumparaturi.xlsx îl vom pune într-o arhiva ZIP pe care o vom cripta cu parolă.

Redenumirea fişierului o realizăm cu click dreapta pe fişier iar din meniu aferent selectăm Rename sau selectăm fişierul şi apăsam la tastatură tasta F2.

Pentru arhivarea fişierului folosim aplicația 7ZIP[53] care este freeware. Tot ce trebuie să facem este să dăm click dreapta pe fişier, selectăm 7-Zip şi Add to archive... Acest lucru ne deschide o fereastră de dialog în care putem specifica nivelul de criptare şi parola.

[53] http://www.7-zip.org/ accesat 06/06/2011

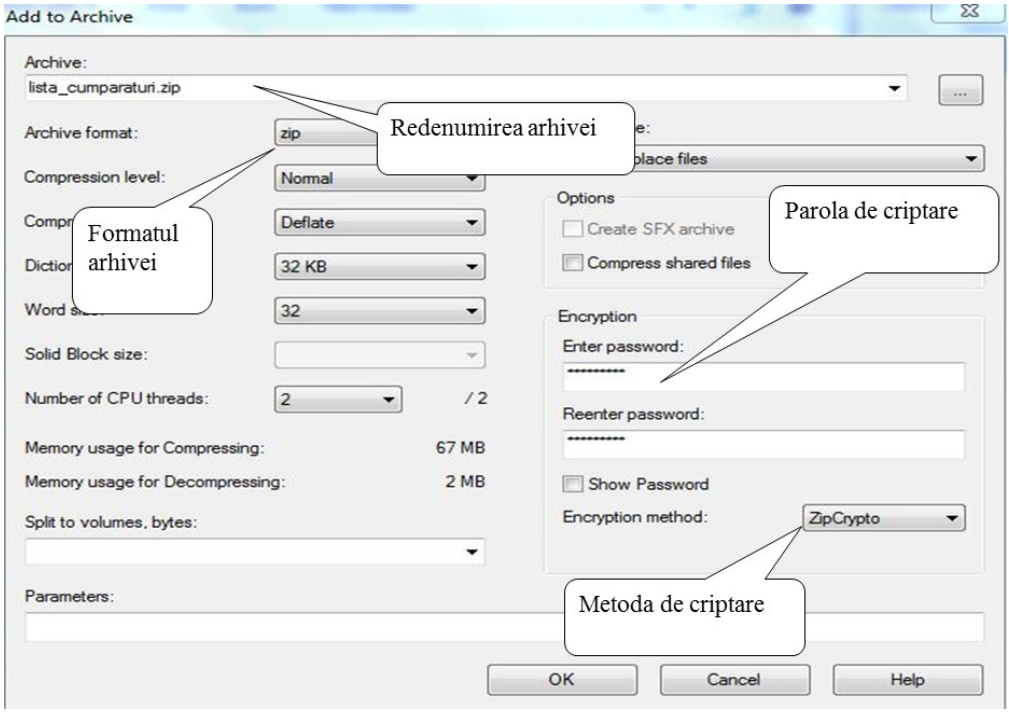


Figura nr. 12.1 – *Arhivarea cu 7ZIP*

În imaginea de mai sus avem caseta de dialog la crearea unei arhive ZIP cu opțiune de criptare.

Acum că am creat arhiva respectivă ar fi bine să o redenumim de exemplu joc.zip. Acest lucru ne va ajuta la pasul următor.

Pasul 2 Schimbarea extensiei arhivei

O arhivă poate da de bănuit atunci când stickul pe care se află este supus unei investigații digitale. Pentru a ne masca şi mai bine fapta, în continuare, vom schimba extensia arhivei din ZIP în EXE. Un ochi ne-experimentat care se uită la acest așa-zis executabil, dacă va da dublu click pe el va întâmpina o eroare de sistem, va crede că executabilul este corupt şi va trece peste o analiză mai amănunțită a acestuia.

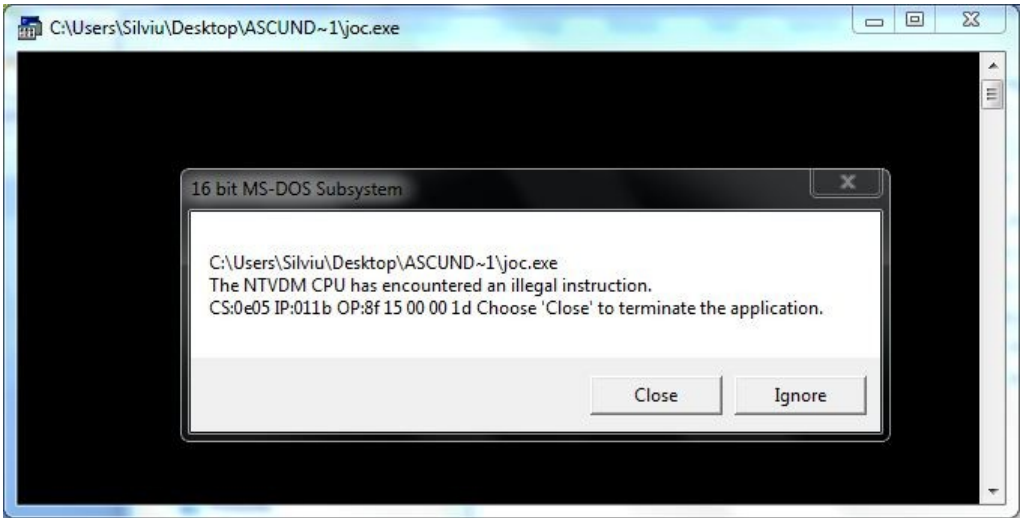

C:\Users\Silviu\Desktop\ASCUND~1\joc.exe
16 bit MS-DOS Subsystem
C:\Users\Silviu\Desktop\ASCUND~1\joc.exe
The NTVDM CPU has encountered an illegal instruction.
CS:0e05 IP:011b OP:8f 15 00 00 1d Choose 'Close' to terminate the application.
Close
Ignore

Figura nr. 12.2 - *Eroare la rularea executabilului joc.exe*

Imaginea de mai sus demonstrează eroare obținută când este rulat executabilul „fantomă".

Pentru a avea acces la extensia unui fişier şi pentru a o putea modifica trebuie să debifăm opțiunea *Hide extensions for known file types* din *Folder Options*. După ce a fost debifată această opțiune, când încercăm să redenumim fişierul, vom avea acces şi posibilitatea de a schimba extensia.

Pas 3 Folosirea unui editor de HEX pentru schimbarea amprentei arhivei ZIP

Unui investigator cu ceva experiență i se va părea ciudat acest executabil care nu rulează şi ar putea face o analiză a tipului de fişier pentru a afla dacă într-adevăr este vorba de un executabil. Folosind un editor de hex, XV32, observăm că numărul magic (semnătura digitală a fişierului) al unei arhive de tip ZIP este „50 4B" iar pentru un fişier executabil „4D 5A". În imaginea de mai jos sunt prezentate astfel de semnături digitale.

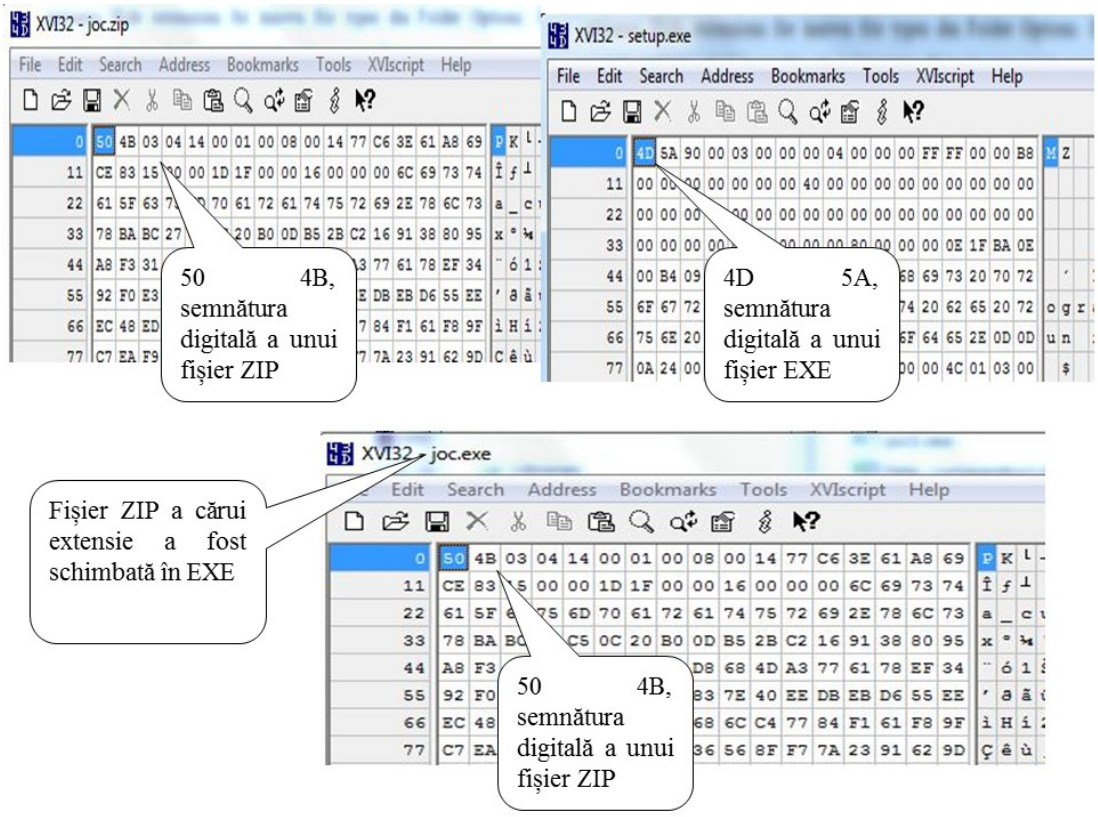

XVI32 - joc.zip
File Edit Search Address Bookmarks Tools XVIscript Help
50 4B, semnătura digitală a unui fişier ZIP
XVI32 - setup.exe
File Edit Search Address Bookmarks Tools XVIscript Help
4D 5A, semnătura digitală a unui fişier EXE
Fişier ZIP a cărui extensie a fost schimbată în EXE
XVI32 - joc.exe
Edit Search Address Bookmarks Tools XVIscript Help
50 4B, semnătura digitală a unui fişier ZIP

Figura nr. 12.3 - *Semnăturile digitale ale fişierelor de tip ZIP şi EXE*

Chiar dacă am schimbat extensia din ZIP în EXE se poate observa că „numărul magic" a rămas cel al unui fişier ZIP. În continuare tot ce trebuie să facem este să editǎm 50 4B în 4D 5A şi să apăsăm butonul de salvare. Rezultatul va arăta ca în figura de mai jos.

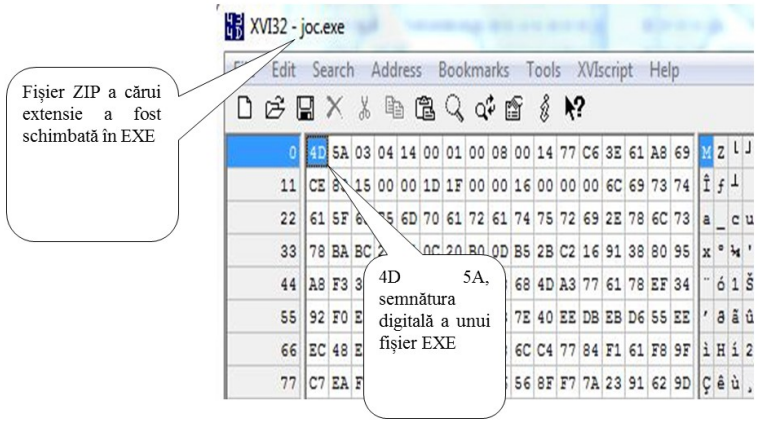

XVI32 - joc.exe
Edit Search Address Bookmarks Tools XVIscript Help
Fişier ZIP a cărui extensie a fost schimbată în EXE
4D 5A, semnătura digitală a unui fişier EXE

Figura nr. 12.4 - *Semnătura digitală a unui fişier ZIP a cărui număr magic a fost modificat*

Acum pe lângă faptul că arată ca un fişier executabil şi sistemul de operare Windows îl vede ca pe o aplicaţie, un ochi neexperimentat va putea fi păcălit uşor de această schimbare a „numărului magic”.

Figura nr. 12.5 - *SO Windows „vede” fişierul ca pe o aplicaţie*

Pentru o persoană cu suficiente cunoştinţe din domeniul IT o astfel de modificare a unui fişier nu ia mai mult de 10 minute. Ultimul lucru care a rămas de făcut este ascunderea stickului de memorie pe care păstrăm fişierul.

12.2. Partea II – Colectarea, analiza, păstrarea şi prezentarea probelor digitale

În partea a 2-a a acestei lucrări practice jucăm rolul unui investigator de echipamente digitale, specialist ce va face analiza tehnico-ştiinţifică a echipamentul bănuit că ar conţine probe incriminatorii. Din nefericire, în România, legislaţia nu este foarte cuprinzătoare cu privire la astfel de anchete iar standardele internaţionale de care vorbeam în capitolul 1 nu sunt adoptate şi nici nu am găsit proiecte de legi care să reglementeze alinierea la astfel de standarde.

În continuarea voi încerca să imaginez o investigare a echipamentului suspect ţinând cont atât de Codul de Procedură Penală cât şi de ceea ce este recomandat în standardele internaţionale.

Pasul 1 Ridicarea mijloacelor materiale de probă. Efectuarea percheziţiei

Codul de procedură penală defineşte mijlocul material de probă în *Secţiunea VII, Art. 94* astfel: „Obiectele care conţin sau poartă o urmă a faptei săvârşite, precum şi orice alte obiecte care pot servi la aflarea adevărului, sunt mijloace materiale de probă.”. Până să devină însă mijloc de probă în instanţă, mijlocul material este doar un corp delict aşa cum este definit în *Art. 95* al aceeaşi secţiuni VII: „Sunt, de asemenea, mijloace materiale de probă obiectele care au fost folosite sau au fost destinate să servească la săvârşirea unei infracţiuni, precum şi obiectele care sunt produsul infracţiunii.”.

Până la ridicarea corpului delict însă, conform Codul de procedură penală, trebuie efectuată o percheziţie la domiciliul inculpatului care poate fi dispusă doar de judecător în cursul urmăririi penale. În cazul nostru, pentru a evita alertarea inculpatului şi o eventuală distrugere a corpului delict, inculpatul va fi urmărit penal fără citarea părţilor. Acest lucru este reglementat în *Art 100* al *Secţiunii VIII*, *Al 3* şi *Al 4*. Modul în care trebuie efectuată percheziţia este reglementat în *Art. 105*.

Odată începută percheziţia, articolele 107, 108, 109 şi 110 reglementează identificarea şi păstrarea obiectelor şi mijloacelor materiale care vor constitui probe, procesul-verbal de percheziţie şi ridicare a obiectelor şi măsurile şi modalităţile de conservare a probelor. Din nefericire legislaţia română nu cuprinde referinţe la modul de stocare a mijloacelor de probă care să conţină probe digitale şi nici nu precizează cum trebuie manipulate astfel de probe. Aici intervin standardele internaţionale care deşi nu sunt precizate sau acceptate în nici un act oficial garantează un cadru de lucru care să ducă la găsirea de dovezi imposibil de contestat.

După efectuarea percheziţiei, găsirea stickului de memorie, corpului delict ce face subiectul lucrării de faţă, şi sigilarea sa într-un plic sau conform standardelor internaţionale într-un recipient care să ferească stickul de memorie de acţiunea câmpurilor electro-magnetice şi transportarea şi depozitarea în vederea analizei, teoretic ar trebui să avem deja acel lanţ de custodie care atestă toate acţiunile şi toate persoanele care au intrat în contact cu acest corp delict de la găsirea acestuia până la analiză.

În România acest document singular care să prezinte traseul stickului de memorie nu există, cel puţin nu este reglementat legal. În schimb există un proces verbal care atestă găsirea şi ridicarea

obiectelor. *Secțiunea V. Înscrisurile* din Codul de procedură penală reglementează procesul-verbal ca mijloc de probă şi cuprinsul şi forma acestuia. *Art. 108* al *Secțiunii VIII* completează cu datele ce trebuiesc notate la percheziție şi ridicarea obiectelor de probă şi anume locul, timpul şi condițiile în care înscrisurile şi obiectele au fost descoperite şi ridicate, enumerarea şi descrierea lor amănunțită, pentru a putea fi recunoscute.

Procesul-verbal care atestă găsirea şi ridicarea stickului de memorie poate fi văzut în Anexa1.

Pasul 2 Pregătirea mediului de lucru şi analiza corpului delict

Subiectul analizei cuprinse în această lucrare îl face stickul de memorie pe care am ascuns fişierul incriminatoriu aşa că ne vom concentra asupra acestuia. Aşadar în procesul verbal de constatare a fost cuprins acest stick de memorie care a fost găsit ascuns într-un şifonier, într-un loc greu accesibil sau văzut, împreună cu pozele aferente. Pe acest stick nu sunt vizibile decât marca Verbatim şi un număr 08091101304G31AAD. Stickul de memorie a fost pus spre păstrare într-un plic sigilat şi transportat la sediu unde urmează să fie supus la o serie de procedee ce vor permite analiza. Jurnalul investigatorului poate fi văzut în Anexa 2.

Pasul 2.1 Blocarea la scriere a echipamentelor de stocare

Odată ce corpul delict a ajuns în posesia investigatorului poate începe constatarea tehnico-ştiințifică descrisă sumar în Codul de procedură penală, *Secțiunea IX Constatarea tehnico-ştiințifică şi constatarea medico-legală* dar, mai întâi, trebuie să asigurăm un mediu de lucru care nu va modifica în nici un fel corpul delict, compromițând astfel integritatea dovezii. În primul rând trebuie să ne asigurăm că în momentul în care conectăm stickul de memorie la calculator, acesta nu va fi modificat. În momentul în care conectăm un astfel de dispozitiv la calculator este modificat fişierul de configurare a acestuia cu data şi ora ultimei accesări. Pentru a evita acest lucru, pe sistemele Windows (nu este cazul pe sistemele Linux), trebuie instalat un program/aplicație care să blocheze scrierea stickurilor de memorie dar, să permită citirea. Pentru aceasta putem folosi o aplicație precum Thumbscrew USB Write Blocker. Este o aplicație freeware foarte uşor de folosit dar, din păcate nu garantează 100% blocarea stickului de memorie la scriere. Pentru a realiza o investigație digitală care să elimine orice urmă de îndoială este recomandată folosirea unui software plătit, cu licență, care să garanteze blocarea scrierii pe stickuri de memorie. Din testele realizate Thumbscrew USB Write Blocker s-a dovedit a fi de încredere dar, am ales o metodă care să aducă un plus de siguranță.

Pe sistemele Windows, sistem folosit de altfel în această investigație, blocarea scrierii pe stickuri de memorie poate fi realizată din regiştrii calculatorului

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect

Pe multe maşini este posibil ca WriteProtect să nu existe. În acest caz îl vom crea noi înşine astfel:

1. Deschidem Registry Editor (Run > regedit)
2. Navigăm până la HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
3. Creăm o cheie nouă (Edit > New > Key) pe care o denumim StorageDevicePolicies
4. Selectăm cheia StorageDevicePolicies şi apoi creăm o nouă valoare DWORD (32-bit) (Edit > New > DWORD (32-bit) value) pe care o denumim WriteProtect
5. Dublu click pe WriteProtect şi setăm Value Data 1 ca în imaginea de mai jos. Implicit aceasta are valoarea 0.

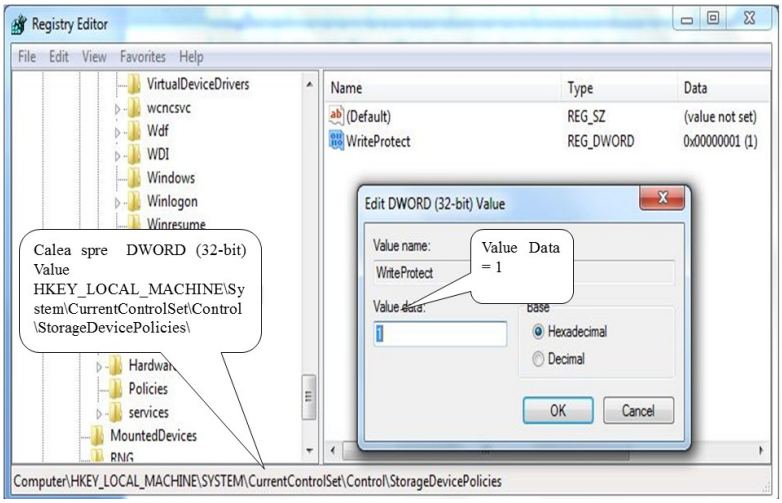


Figura nr. 12.6 - *Modificarea registrilor calculatorului pentru a bloca scrierea stickurilor de memorie*

Imaginea de mai sus arată crearea valorii WriteProtect şi modificarea acesteia pentru a bloca scrierea.

Pasul 2.2 Calculul „amprentei digitale" şi clonarea corpului delict

Acum că am blocat scrierea stickului de memorie şi implicit modificarea lui putem trece mai departe şi anume calcularea unei sume de control, valoarea hash care acţionează ca o amprentă digitală a stickului, identificând-ul unic. Orice modificarea cât de mică asupra echipamentului şi valoarea hash se va schimba indicând astfel că probele au fost compromise. Pentru acest lucru avem nevoie de un software specializat aşa că am ales FTK Imager 3.0.1[54] de la Access Data.

Cu ajutorul funcţiei Verify Drive/Image putem obţine un raport preliminar asupra stickului de memorie, în acest raport fiind inclusă valoarea hash MD5.

[54] http://accessdata.com/downloads/current_releases/imager/FTKImager_UserGuide.pdf accesat 10/06/2011, ora 12:33

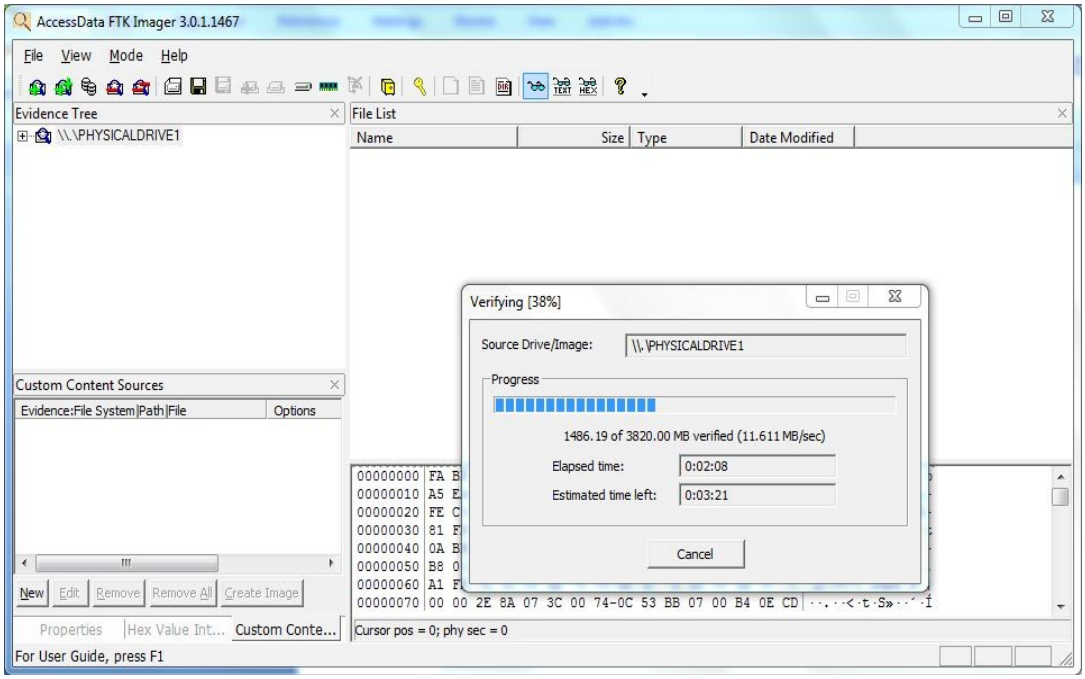


Figura nr. 12.7 - *Calculul valorii MD5 inițiale cu FTK Imager*

Valoarea MD5 este prezentată în figura următoare:

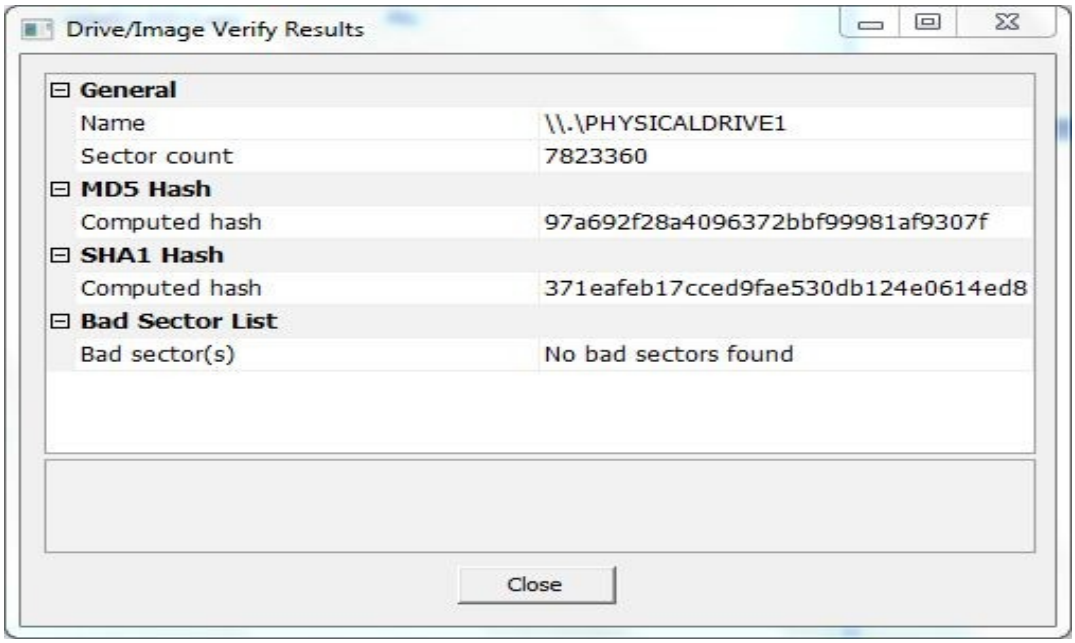


Figura nr. 12.8 - *Valoare MD5 stick memorie*

Valoarea MD5 rezultată este 97a692f28a4096372bbf99981af9307f.

De asemenea putem scoate o lista cu directoarele de pe stickul de memorie ce ne va ajuta în căutarea unor fişiere cu valoare în incriminarea suspectului inclusiv documente şterse de curând. Acest lucru poate fi realizat cu funcția Export Directory Listing.

Acum că am calculat valoarea hash a echipamentului putem merge mai departe şi să îl clonăm. Analiza se face pe clonă nu pe echipamentul incriminat.

Ca mod de creare a unei clone am ales opțiunea Create Image din FTK Imager cu formatul imaginii AFF (Advanced Forensics Format) deoarece putem realiza imagini comprimate sau nu, deci nu avem restricție la mărimea imaginii, poate fi extinsă, este open source, poate fi verificată pentru consistență, imaginea poate fi segmentată şi este o copie la nivel de bit a echipamentului fizic.

Înainte de crearea imaginii am bifat opțiunea de creare a unei liste cu directoarele conținute pentru o eventuală comparație cu prima astfel de listă obținută.

De asemenea înaintea creării imagini ni se cer câteva informații legate de cazul curent precum numărul cazului, numărul probei, descriere unică, numele examinatorului.

Din sumarul creării imaginii se poate observa că valoarea hash MD5 este identică cu prima valoare MD5 calculată asupra stickului de memorie. Raportul complet poate fi observat în Anexa3.

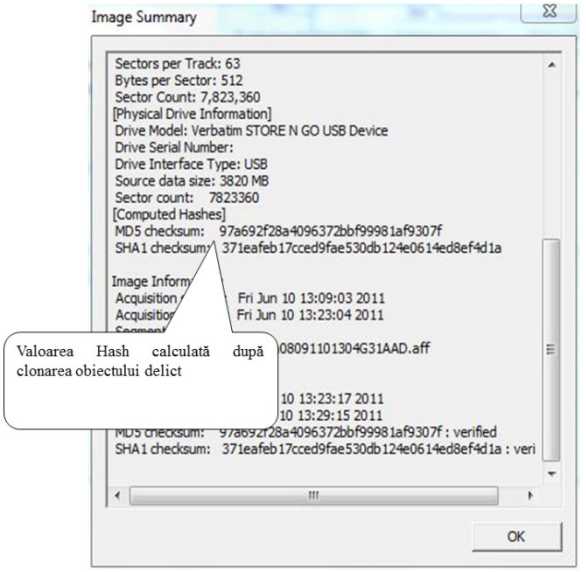


Figura nr. 12.9 - *Valoarea MD5 după clonare*

Pasul 2.3 Analiza clonei şi identificarea probelor digitale

Primul pas în analiza clonei este folosirea funcției Mount din FTK Imager care ne va permite să vedem corpul delict ca pe o nouă partiție la sistem.

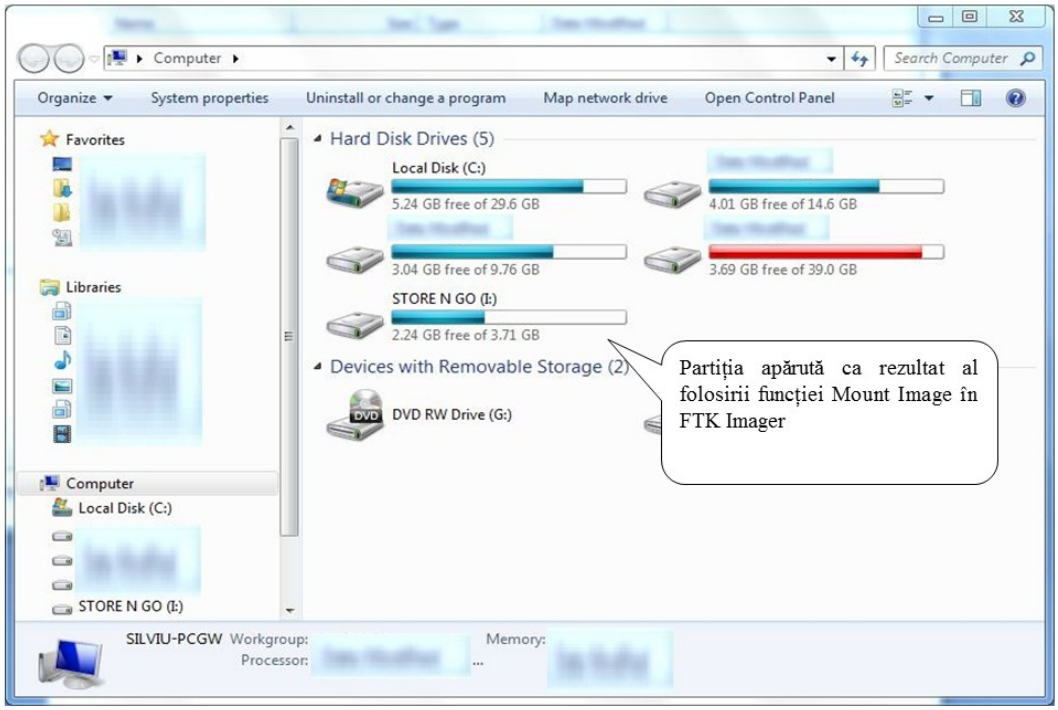


Figura nr. 12.10 - *Montarea imaginii cu FTK Imager*

Noua partiție este o copie fidelă a stickului de memorie. După cum se poate observa are aceeaşi
denumire şi capacitate ca stickul fizic.

Următorul pas este investigarea fişierelor care se găsesc în imagine. Se foloseşte un software profesional precum Forensic Tool Kit (FTK 3.3) de la Access Data care este foarte apreciat în SUA sau EnCase pentru analiza tipurilor de fişiere. Din păcate aceste instrumente software sunt foarte scumpe de achiziționat şi nu există variante demo sau programe de test pentru studenți care doresc să facă cercetare în acest domeniu. Principiul folosit este relativ simplu, se iau toate fişierele din imagine şi se analizează în profunzime pentru a descoperi dacă nu ascund ceva în spate.

Listarea directoarelor pe care am făcut-o atât la începutul cât şi după ce am creat imagine ne ajută la descoperirea fişierelor şterse deoarece evidențiază astfel de fişiere. Desigur pentru recuperarea acestora ar trebui să folosim unu instrument la fel de inaccesibil ca şi celelalte menționate mai sus.

Reluăm lucrarea şi presupunem că analiza fişierelor cu unul din instrumentele de mai sus a dat roade şi am identificat fişierul joc.exe ca fiind de fapt o arhivă ZIP. Arhiva este criptată cu parolă, iar pentru a trece de acest impediment vom folosi un alt instrument software de la Access Data care de această dată poate fi folosit în varianta demo şi putem sparge parole pentru fişiere de tip ZIP. Instrumentul ales este Password Recovery Tool Kit. Tot ce trebuie să facem este să selectăm fişierul criptat, să specificăm numele cazului şi să pornim procesul de decriptare. La finalizarea acestuia avem ca rezultat parola „Garfield” .

Ultimul lucru pe care investigatorul trebuie să îl facă este să deschide arhiva şi să întocmească un proces verbal cu rezultatele analizei tehnico-ştiințifice.

Capitolul 13. Studiul de caz 2 - Accesarea probelor pe niveluri

În acest studiu de caz ne propunem să punem la dispoziția cititorului o metodă sau un scurt îndruma de acces la probele digitale stocate pe un calculator Windows.

Cazul pleacă de la ideea că un anumit calculator este protejat pe mai multe niveluri şi că s-a realizat deja accesul fizic la dispozitivul suspect.

Investigatorul trebuie să aibă acces la un fişier protejat de pe discul care este criptat cu EFS.

Nivelurile de protecție pe care le putem asigura unui calculator sunt:

- Accesul la BIOS
- Accesul în sistemul de operare
- Accesul la fişiere
- Accesul la jurnale
- Accesul al arhive protejate.

Cea mai comună metodă de protecție este utilizarea parolelor pe fiecare din nivelurile enumerate anterior. În mare parte infractorii IT profesionişti folosesc multe alte niveluri de protecție, mergând din ce în ce mai mult pe protecția biometrică sau pe păstrarea datelor în alte locații decât dispozitivul fizic de pe care se lucrează, sau chiar utilizarea unor dispozitive de unică folosință.

Accesul fizic la calculator

La ora actuală având în vedere că majoritatea dispozitivelor de calcul sunt conectate într-un fel sau altul al Internet, iar dispozitivele, locațiile şi metodele de acces la Internet sunt foarte variate, identificarea unui dispozitiv fizic poate fi un proces destul de anevoios, care implica de cele mai multe ori o serie de proceduri speciale de identificare şi mai ales de realizare corectă a trasabilității unui pachet de date care circulă pe internet.

În această procedură intervin de cele mai multe ori organele de cercetare penala care solicită în scris operatorilor de servicii de internet acces la bazele de date cu înregistrările de trafic, în vederea identificării corecte a făptuitorului unei fapte.

Sunt mai multe elemente prin intermediul cărora se pot identifica dispozitivele fizice suspecte: Adresa IP, Codul abonat de la furnizorul de Internet, Adresa fizică a calculatorului, alte elemente de identificare a traficului.

Accesul la secvența de boot

După ce un dispozitiv de calcul suspect a fost identificat trebuie conservat, dar înainte de aceasta trebuie clonat pentru a putea să analizăm datele şi să identificăm potențialele probe fără a afecta conținutul original al dispozitivului de calcul.

În cazul în care nu deținem instrumente de clonare a hard-discurilor direct ataşate, putem folosi alternativa pornirii calculatorului prin utilizarea unui CD specializat cu ajutorul căruia să accesăm fişiere, jurnale sau alte informații din sistemul de operare fără a ajunge la acesta.

BIOS-ul este acronimul expresiei engleze Basic Input/Output System, o componentă software de bază a calculatoarelor (PC-uri şi servere) care face legătura între componentele fizice (hardware) şi sistemul de operare utilizat pe calculatorul respectiv.

Câteva dintre companiile producătoare de BIOS-uri sunt: Award, American Microsystems, Inc. (AMI) şi Phoenix Technologies Ltd. (Phoenix).

BIOS-ul îndeplineşte trei funcţii fundamentale:

1.Verificarea componentelor la pornirea calculatorului (Power On Self-Test sau POST)

2.Încărcarea sistemului de operare de pe discul dur (HDD) în memoria de lucru

3.Face legătură între sistemul de operare şi unele dispozitive fizice

Pe lângă funcţiile fundamentale BIOS-ul are rolul de proteja secvența de bootare a calculatorului prin specificarea dispozitivelor de pe care se face bootarea.

Calculatorul unei companii trebuie să permită bootarea numai de pe hardisk pentru a preveni eventualele tentative de a boota calculatorul cu ajutorul unei disckete, CD sau momory stik.

Pentru a preveni schimbarea secvenței de bootare BIOS-ul poate fi protejat cu o parolă. Scopul nostru în această etapă este să depăşim această parolă.

Metoda 1: Parola implicită

În funcție de tipul producătorului BIOS-ului putem încerca o serie de parole implicite. Detalii: http://www.elfqrin.com/docs/biospw.html

Metoda 2: Eliminarea bateriei de pe placa de bază

Pentru a putea păstra în memorie setările utilizator (parola, secvența de boot) cipsetul care stochează aceste informații are nevoie de o baterie care se află pe placa de bază a calculatorului. Eliminarea acestei baterii produce invariabil revenirea tuturor setărilor BIOS la parametrii de fabrică care nu conțin o parolă de acces la BIOS.

Odată resetată parola de BIOS putem avea acces şi să modifică secvența de Boot. Putem în acest fel boota cu un CD specializat sau un memory stik pentru a realiza clonarea hardiscului şi analiza datelor de pe acesta.

Accesul la sistemul de operare

Chiar dacă este o imagine clonată sau un calculator de sine stătător, pentru a putea să accesă fişierele trebuie să ne autentificăm pe calculator prin folosirea numelui de utilizator şi a parolei. Pe un calculator pot exista mai mulți utilizatori înregistrați, şi pentru a accesa corect fişierele stocate de un anumit utilizator trebuie să folosim privilegiile acestuia sau privilegii de administrator.

În cazul în care nu cunoaştem nici una din parole, trebuie să accesăm altfel fişierele sau să încercăm o recuperare a parolei prin utilizarea unor programe specializate.

De asemenea, pentru a putea să recuperăm fişiere şterse de pe discuri, în sensul ascunderii urmelor, trebuie să ne conectăm la sistemul de operare, clonare nefiind suficientă.

Hiren's BootCD[55] este unul din cele mai cunoscute produse destinate resetării parolelor uitate sau a creării de imagini a discurilor. El presupune bootarea calculatorului cu ajutorul acestui CD şi utilizarea instrumentelor specifice de resetare a parolelor.

În continuare vom prezenta câteva din facilitățile şi instrumentele puse la dispoziție de Hiren's BoodCD.

Hiren's BootCD este un Live CD **Botabil** ce conține o serie de aplicații care acoperă o paleta larga de utilitare pentru testarea diverselor componente PC, recuperări de date ce survin din ştergerea accidentala a fişierelor sau din ştergerea partițiilor, utilitare pentru scanarea si repararea

[55] http://www.hirensbootcd.org/

hardurilor cum ar fi “HDD Regenerator”, dar si programe ce ofera posibilitatea partitionarii hard discurilor, precum si testarea lor, şi nu doar atat.

Acest utilitar contine si **Mini Windows Xp** acesta este o versiune mai mica a lui Windows XP pe care insa nu e nevoie sa o instalam pe calculator, sistemul de operare va rula in momentul cand selectam aceasta optiune, de pe cd, el punand fisierele de care are nevoie in memoria RAM, iar apoi Windows-ul va rula in mod normal. Accesarea acestui utilitar se face din meniul de botare a cd-ului dupa care acesta se va afisa ca un Windows XP normal.

În continuare vom prezenta o listă de instrumente utile pentru activitatea investigatorilor:

Utilitare de creare a imaginilor

- Partition Saving 3.71: Un utilitar pentru backup/restore a partitiei. (SavePart.exe).
- COPYR.DMA Build013: Un utilitar pentru a face copia unui hard ce are sectoare cu baduri.
- ImageCenter 5.6 (Drive Image 2002): soft pentru clonarea hardurilor.
- Norton Ghost 11.5: Similar cu Drive Image (cu support pentru usb/scsi).
- Acronis True Image 8.1.945: Creaza o imagine exacta a discului pentru un backup complet al sistemului
- DriveImageXML 2.02: Face backup pentru orice hard-disk/partitie catre un fisier de tip imagine chiar daca discul este in folosinta
- Drive SnapShot 1.39: creaza o imagine de disc a sistemului de operare intr-un fisier in timp ce sistemul de operare functioneaza
- Ghost Image Explorer 11.5: pentru a adauga/sterge/extrage fisiere de pe un fisier de tip imagine Ghost
- DriveImage Explorer 5.0
- WhitSoft File Splitter 4.5a.
- Express Burn 4.26
- Smart Driver Backup 2.12
- Double Driver 1.0: Driver Backup si Restore .
- DriverBackup! 1.0.3:

Utilitare de recuperare de date

- Active Partition Recovery 3.0: Recupereaza o partitie stearsa
- Active Uneraser 3.0: Pentru recuperarea fisierelor sterse si a dosarelor sterse de pe partitii de tipul FAT si NTFS .
- Ontrack Easy Recovery Pro 6.10: Pentru recuperarea datelor ce au fost sterse.
- Winternals Disk Commander 1.1:
- TestDisk 6.11.3: Utilitar pentru a verifica si a reface partitiile
- Lost & Found 1.06: Un vechi si bun utilitar pentru recuperarea datelor.
- DiyDataRecovery Diskpatch 2.1.100:
- Prosoft Media Tools 5.0 v1.1.2.64:
- PhotoRec 6.11.3: Program ce permite recuperarea fisierelor sau a pozelor
- Winsock 2 Fix for 9x:
- XP TCP/IP Repair 1.0:
- Active Undelete 5.5: un utilitar pentru recuperarea fisierele sterse.
- Restoration 3.2.13:
- GetDataBack for FAT 2.31: Recuperarea datelor de pe partitii de tipul FAT.
- GetDataBack for NTFS 2.31: Recuperarea datelor de pe partitii de tipul NTFS.

- Recuva 1.27.419: Restaureaza fisierele sterse de pe Hard-diskuri , Camere digitale Memory Carduri, usb mp3 player…
- Partition Find and Mount 2.3.1: Este facut pentru a identifica partitiile sterse sau pierdute.
- Unstoppable Copier 4b: permite copierea fisierelor de pe diskuri cu probleme cum ar fi bad sectors, zgarieturi sau care dau erori la citirea normala

Utilitare pentru eliminarea diverselor parole Windows

- Active Password Changer 3.0.420: Este un utilitar pentru restetarea parolei de utilizator in Windows NT/2000/XP/2003/Vista (FAT/NTFS).
- Offline NT/2K/XP Utilitar pentru schimbarea parolei de administrator/utilizator pentru windows nt/2000/xp
- Registry Reanimator 1.02:
- NTPWD: Utilitar pentru schimbarea parolei de administrator/utilizator pentru windows nt/2000/xp.
- Registry Viewer 4.2:Editeaza registrii
- ATAPWD 1.2: Utilitar pentru parola de Hard Disk.
- TrueCrypt 6.2:
- Content Advisor Password Remover 1.0:
- Password Renew 1.1: Utilitar pentru resetarea parolei de Windows.
- WindowsGate 1.1:
- WinKeyFinder 1.73:
- XP Key Reader 2.7: Poate decoda XP-keyul.
- ProduKey 1.35:
- Wireless Key View 1.26:
- MessenPass 1.24:
- Mail PassView 1.51.

Produse din aceeaşi categorie:

- BartPE (http://www.nu2.nu/pebuilder/)
- Active@ Boot Disk (http://www.livecd.com/)
- UBCD4WIN (http://www.ubcd4win.com/)

Odată intrați în sistemul de operare putem identifica fişierele de care avem nevoie pentru probe sau putem consulta jurnalele de activități pentru vedea firul de execuție a unei oprațiuni efectuate de utilizator.

Accesul la fişiere

Accesul la fişiere este relativ simplu odată intrați în sistemul de operare. Totuşi anumite fişiere pot fi şterse pentru a elimina probele. În acest caz trebuie să utilizăm aplicații specializate ca cele prezentate în secțiunea anterioară.

Accesul la jurnale

Event Viewer

Aplicația de vizualizare a mesajelor despre diferite evenimente) include 3 categorii implicite de înregistrări:

- monitorizarea mesajelor de la aplicațiile instalate

- monitorizarea mesajelor de securitate
- monitorizarea mesajelor de sistem

Pentru a vizualiza un mesaj în mod detaliat trebuie deschis prin dublu click. Există trei tipuri de mesaje: *Information* (mesaje de informare), *Warning* (mesaje de alarmă) şi *Error* (mesaje de eroare).

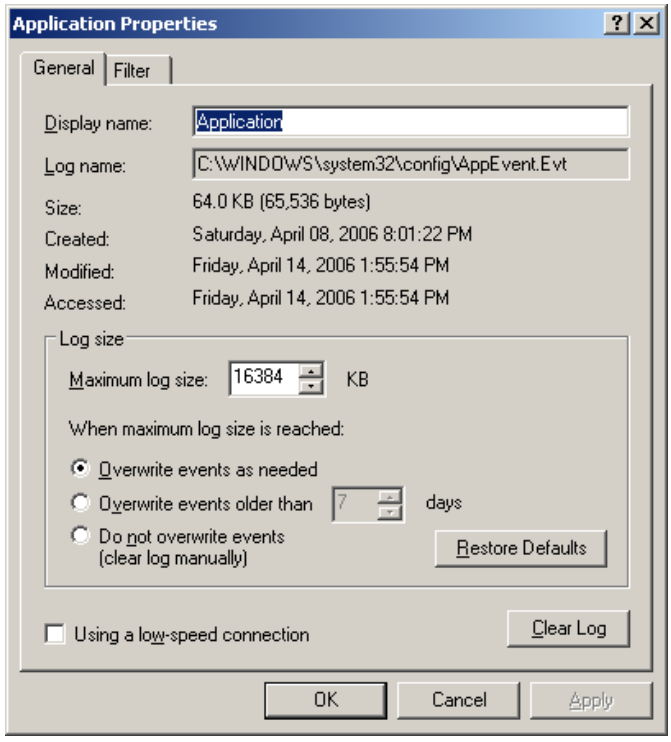


Figura nr. 13.1 - *Fereastra de proprietăți a unei categoriei de mesaje Application.*

Fiecare categorie din *Event Viewer* poate fi parametrizată click dreapta al mouse-ului pe ea şi alegerea opțiunii **Properties** din meniul contextual afişat.

Principalele opțiuni sunt:

- *Maximum log size* (mărimea maximă a fişierului care stochează înregistrările) – exprimat în Kb. Vă recomandăm să măriți de 2-3 ori capacitatea de stocare a fişierului respectiv pentru fiecare categorie în parte;
- Acțiunea care se va efectua în momentul în care fişierul de log a ajuns la dimensiunea maximă unde putem alege: suprascrierea evenimentelor dacă este nevoie (*Overwrite events as needed*); suprascrierea evenimentelor mai vechi de 7 zile; ştergerea manuală a înregistrărilor;
- Ştergerea cu posibilitatea de salvare a înregistrărilor (butonul *Clear Log*). Înregistrările din Event Viewer pot fi salvate în formatul proprietar ***EVT*** sau în formatul ***CSV*** (*coma separated value*) care permite importul şi analiza informațiilor în aplicații de calcul tabelar şi numai.

Pentru parametrizarea informațiilor care vor fi înregistrate în categoria Security trebuie să accesăm politica de securitate locală a serverului:

1. **Start → Administrative Tools → Local Security Policy**;

2. În fereastra *Local Security Settings* în categoria *Local Policies* activați de la subcategoria *Audit Policy* opțiunile pentru: *Audit account logon events*, *Audit account management*, *Audit logon events*, *Audit policy change*.
3. După efectuarea schimbărilor respective şi închiderea ferestrelor deschise, redeschizând Event Viewer o să constatați că deja au început să apară alte tipuri de înregistrări în *Security*.

Glosar de termeni

ATM: (Asynchronous Transfer Mode). O tehnologie a rețelelor de calculatoare in care conexiunile dintre echipamentele de comunicație sunt setate, folosite si eliminate in mod dinamic.

Backbone: O porțiune a rețelei care suporta traficul cel mai intens; sistemul principal de cabluri care asigura comunicația intre punctele de distribuție precum si comunicația cu camera echipamentelor si punctele de acces in clădire.

Bandwidth: Cantitatea de informații sau date care pot fi trimise printr-o conexiune de rețea într-o perioadă de timp. Lățime de bandă de obicei este declarat în biți pe secundă (bps), kilobiți pe secundă (kbps) sau megabiți pe secundă (mbps).

BIOS: (Basic Input Output System). Setul de rutine stocate în memoria ROM (doar în citire) pe un sistem de circuite de pe placa de bază care porneşte calculatorul prin inițializarea dispozitivelor fizice, apoi transferă controlul sistemului de operare. BIOS-ul deschide canale de comunicare cu componentele calculatorului, cum ar fi hard disk-uri, tastatura, monitor, imprimanta şi porturile de comunicare.

Bit: Binary Digit. Un bit este cea mai mica unitate de informație, constând dintr-o singura cifra binara. Este reprezentat de valorile numerice 1 sau 0.

BMP: Extensie a fişierelor de tip Bitmap, utilizate pentru stocarea imaginilor digitale.

Buffer: Un bloc de memorie care stochează date temporar şi permite acestora să fie citite sau scrise în bucăți mai mari pentru a îmbunătăți performanța unui computer. Buffer-ul este utilizat pentru depozitarea temporară a datelor care se citesc sau sunt în aşteptare pentru a fi trimise către un dispozitiv, cum ar fi un hard disk, CD-ROM, imprimantă, în rețea sau unitate de bandă.

Cadre: Un cadru este grup de biți care constituie un bloc de informație. Cadrul conține informații de control a rețelei sau date. Mărimea si alcătuirea cadrelor este determinata de protocolul de rețea utilizat. Cadrele sunt generate pe nivelul 2 al modelului OSI. (engl.: frame)

CAT-5/Category-5: Cablu de transmitere a datelor cu viteză mare (100 mbps sau mai mult). Cablurile de tip CAT-5 sunt utilizate în special pentru transmiterea de voce şi date.

CAT-5e: (Enhanced CAT-5). Similar cu CAT-5 dar cu o serie de îmbunătățiri.

CAT-6/Category-6 (ANSI/TIA/EIA-568-B.2-1): Un cablu standard pentru rețelele de tip Gigabit sau alte tipuri de interconectări compatibile cu CAT-5, CAT-5e şi Cat-3. Principalele sale specificații sunt orientate către reducerea perturbărilor de transmisie prin rețea.

CD/CD-ROM: (Compact Disc—Read-Only Memory). Un tip de unitate de stocare care conține date şi informații accesibile de un calculator numai pentru citire. Capacitățile standard sunt de 640, 650 sau 700 MB.

CD-R: (Compact Disc—Recordable). Un CD pe care se pot înregistra/scrie date fără a mai putea fi şterse. Se mai foloseşte şi termenul CD-Blank.

CD-RW: (Compact Disc—Rewritable). Un CD pe care se pot scrie, modifica şi şterge date.

Chat Room: O aplicați client pentru anumite tipuri de site-uri web care permit utilizatorilor să comunice în timp real prin utilizarea textului, simbolurilor sau mesajelor audio.

Compact Flash Card: Un dispozitiv de stocare de dimensiuni şi capacități mici, care poate fi îndepărtat de la calculator şi care se bazează pe tehnologia de memorie flash, o tehnologie de stocare care nu necesită o baterie specială pentru a păstra date pe termen nelimitat.

Compressed File: Un fişier a cărui dimensiune este mai mică, de obicei, decât a fişierului original, şi care necesită tehnologii specifice de reducere a dimensiunii prin utilizarea unui algoritm de ştergere sau combinare a informațiilor redundante. Un fişier compresat nu poate fi citit în mod direct de toate aplicațiile până când nu se realizează operațiunea inversă, decompresarea. Se mai întâlneşte şi termenul de arhivare, în momentul în care se utilizează aplicații specializate de compresare: WinZip, WinRar, WinAce etc.

Cookies: Fişiere tip text de dimensiuni mici salvate pe un calculator care stochează informaţii despre site-urile de internet accesate un utilizator.

Copie duplicat bit-cu-bit: Proces de copiere a datelor stocate pe dispozitive digitale, astfel încât copia reproduce datele identic la destinaţie. Termenul de bit-cu-bit referă faptul că datele sunt copiate la nivel de înlănţuire a valorilor care compun sistemul de stocare de la sursă. De exemplu în modul binar reprezintă înşiruirea de 0 şi 1 care compun datele pe mediul de stocare.

CPU: (Central Processing Unit.) Un microcip al calculatorului care conţine de la mai multe mii la mai multe milioane de tranzistori care îndeplinesc mai multe funcţii simultan.

Criptare: Orice procedură utilizată în criptografie pentru a converti un text simplu într-un text cifrat pentru a împiedica pe oricine, în afara destinatarului care are cheia de decriptare corespunzătoare, de la citirea acestor date.

Crosstalk: O perturbare a semnalului electric transmis printr-un cablu UTP sau STP. Crosstalk se referă la faptul că semnalul dintr-un fir sau set de fire afectează semnalul din alt fir sau alt set de fire ale unui cablu.

CSMA/CD: (Carrier Sense Multiple Access with Collision Detection). CSMA/CD este baza sistemului de operare in reţelele Ethernet. Este metoda prin care staţiile urmăresc reţeaua si determina daca sa transmită sau nu date si ce sa facă daca se semnalează o coliziune.

Deleted Files: Fişiere care nu mai au o asociere în tabela de alocare a fişierelor. Fişierele şterse se găsească încă pe mediul de stocare dar nu mai sunt accesibile în mod normal de sistemul de operare.

DHCP: (Dynamic Host Configuration Protocol). Un set de reguli utilizate de echipamentele de comunicare în reţea, precum: calculatoare, rutere, sau altă adaptoare de reţea; permite acestora solicitarea, obţinerea şi utilizarea unei configuraţii TCP/IP de la un server care are o listă de adrese disponibile pentru accesul la reţea sau la Internet.

Digital Camera: Un aparat de fotografiat sau filmat care înregistrează imaginile în format digital. Spre deosebire de camerele analogice care înregistrează un număr infinit de intensităţi ale luminii, camerele digitale înregistrează doar un număr limitat de intensităţi şi salvează datele pe diferite flash card-uri sau discuri optice.

Dispozitiv de stocare electronică: Orice mediu care poate fi folosit pentru a înregistra informaţii pe cale electronică. Exemplele includ hard discuri, benzi magnetice, compact discuri, casete video, casete audio etc. Exemple de dispozitive de stocare amovibile includ unităţi de tip thumb, carduri de memorie, dischete, şi discuri Zip ®.

DivX: Nume al unui set de produse bine cunoscute create de DivX, Inc, inclusiv DivX Codec, care a devenit foarte popular datorită capacităţii sale de a comprima segmente video cu o lungime mare în fişiere de dimensiuni mici, menţinând în acelaşi timp o calitate vizuală relativ ridicată. Ca rezultat, DivX a fost în centrul mai multor controverse datorită utilizării sale în reproducerea şi distribuirea de DVD-uri fără drepturi de autor

Docking Station: Un dispozitiv fizic care permite laptop-urilor şi notebook-urile să folosească echipamente periferice şi componente (scanner, monitor, tastatura, mouse şi imprimante) care în mod normal sunt asociate cu un calculator de birou.

Dongle: O metodă de protecţie împotriva copierii sau un dispozitiv de securitate furnizat odată cu o aplicaţie software.Dongle-ul împiedică utilizarea neautorizată sau duplicarea aplicaţiei software, deoarece fiecare copie a programului necesită un dongle pentru a funcţiona. Mai este cunoscut şi sub numele de cheie HASP sau cheie USB.

Dovada dezincriminatoare: Dovezi care arată că o acuzaţie penală nu este justificată de dovezi.

Driver = aplicaţie software ce permite sistemului de operare să utilizeze în mod optim un sistem hardware.

DSL: (Digital Subscriber Line). O tehnologie de comunicare de mare viteză pentru modemurile digitale utilizate pentru liniile telefonice deja existente.

DVD: (Digital Versatile Disk). Un disc compact de capacitate mare care poate stoca pana la 4,7 Gb (de 28 ori mai mult decât un CD). Tipurile derivate disponibile: DVD-R, DVD-RW, DVD+R, DVD+RW, şi BlueRay.

Ecranaj: Stratul metalic ce protejeaza un cablu de influenta radiatiilor electromagnetice; poate fi alcatuit dintr-o folie sau o plasa metalica ce inveleste cablul pe toata circumferinta. (engl. shield).

EMI: (Electro Magnetic Interference). Este interferenta in semnalele transmise sau receptionate cauzata de cimpurile electrice si magnetice.

Ethernet: O tehnologie din domeniul retelelor de calculatoare care permite ca orice statie dintr-o retea sa transmita la orice moment presupunind ca a verificat traficul pe retea si a asteptat ca reteaua sa fie libera si sa nu existe coliziuni.

Fibra optică: Mediu de transmisie alcatuit din fire de sticla sau plastic invelite intr-un blindaj de protectie din plastic. Fibrele optice transmit informatia sub forma unor fascicole pulsatorii de lumina.

Firewall: Un paravan de protecție (dispozitiv fizic sau aplicație software sau o combinație între fizic şi aplicații) care permite sau blochează traficul în şi dintr-o rețea privată sau calculatorul unui utilizator, si este principala metodă de a ține un calculator securizat de intruşi. De asemenea, este utilizat pentru a separa zona de servere a unei companii de rețeaua sa internă şi pentru a menține segmentele interne de rețea securizate.

FireWire: Un port de comunicație sau bandă de comunicație de mare viteză, serial care permite conectarea a până la 63 de dispozitive. Este utilizat în special pentru descărcarea de informații video de pe camerele video digitale la un calculator.

Firmware: Instructiuni soft care care permit ca un echipament sa functioneze.

Fişier: O colectie de date, informatii inrudite, asociate (engl.: file).

Formatul fişierului: Se referă la tipul de fişier bazat pe structura fişierului, aspect, sau modul în care un anumit fişier are organizate informațiilor (sunete, cuvinte, imagini) conținute în acesta. Formatul unui fişier este indicat de obicei prin extensia de trei sau patru litere: .exe, .doc, .jpg, .html.

GIF: (Graphics Interchange Format). Una din cele mai comune formate de fişiere utilizate pentru stocarea imaginilor. Este utilizat foarte mult pentru paginile de Internet datorită ratei mari de compresie şi faptului că ocupă un spațiu mai mic pe disc decât formatul jpg.

GPS: (Global Positioning System) Un sistem de sateliți şi dispozitive de recepție folosite pentru a calcula pozitiile de pe Pamant. GPS-ul este utilizat în navigare şi orientare, în domeniul afacerilor imobiliare şi topografierea parcelelor de pământ.

Hard Copy: O reproducere permanentă a datelor pe orice media adecvat, pentru utilizarea directă către o persoană, de exemplu, pagini tipărite şi pagini de fax.

Hard Drive: (HDD) Un dispozitiv de stocare a datelor care este compus dintr-un circuit extern, fişe de date şi cabluri de alimentare cu energie electrică; la interior are un strat ceramic de protecție şi platane de metal cu proprietăți magnetice pentru stocarea datelor. Cele mai comune tipuri sunt: IDE, SCSI, SATA, SAS, etc.

Hardware: Componentele fizice care compun un calculator incluzând: tastatura, mouse, monitor şi unitatea centrală.

Header: (ro: Antet) În mai multe discipline de informatică, un antet este o unitate de informații care precede un set de date. Într-o rețea de transport, un antet face parte din pachetele de date şi conține informații transparente cu privire la fişier sau despre transportul de date efectuat. In gestiunea fişierelor, un antet este o regiune la începutul fiecărui fişier în care sunt păstrate date despre acesta. Antetul fişierului poate conține data la care fişierul a fost creat, data la care a fost actualizat ultima dată, şi dimensiunea fişierului. Antetul poate fi accesat numai de către sistemul de operare sau de programe specializate.

Hidden Data (Date ascunse): Multe sisteme informatice includ o opțiune de a proteja anumite informații de utilizatorii ocazionali, prin ascunderea acestora. O examinare sumară a sistemului nu poate afişa fişierele ascunse, directoare, sau partiții pentru utilizatorul neinstruit. O examinare efectuată de un expert va documenta prezența acestui tip de informații.

Host: Un echipament de retea care actioneaza ca sursa sau destinatie a informatiei din retea.

IANA: (Internet Assigned Numbers Authoryty). Agentia care desemneaza si distribuie adresele IP şi nu numai.

IM: (Instant Messenger). Un serviciu de comunicare care permite utilizatorilor să comunice sincron în timp real pe Internet. Este asemănător unei comunicații telefonice numai că se bazează pe scriere nu pe voce. Cele mai cunoscute aplicații pentru IM sunt: Yahoo Messenger, MSN Live Messenger, Google Talk. La ora actuală comunicația prin voce îşi face din ce în ce mai mult simțită prezența, una din cele mai cunoscute aplicații pentru comunicațiile bazate pe voce fiind Skype.

IP: Un număr de 32 di biți care identifică în mod unic un host de pe Internet. Este asociata de administratorul de retea unei anumite interfete de retea. Alocarea adreselor este gestionata de catre agentia internationala IANA. Exemple de adrese: 127.0.0.1, 192.168.1.1, 10.10.1.254.

ISDN: (Integrated Services Digital Network). O linie de comunicații de mare viteză care se bazeaza pe liniile telefonice obişnuite pentru conectarea la Internet.

ISP: (Internet Service Provider). Un tip de afacere economică bazat pe furnizarea serviciilor de acces la Internet, precum şi alte servicii corelate: găzduire de site-uri web, servere de e-mail si altele.

JPG: (Joint Photographic Experts Group – sau JPEG). O tehnică de compresare a imaginilor digitale şi de stocare a acestora. Este foarte utilizat datorită algoritmului de reducere a dimensiunii fişierului fără a afecta foarte mult calitatea imaginii.

LAN: (Local Area Network). O retea locala ca intindere geografica.

MAC (adresa MAC - Media Access Control): Cunoscut şi ca adresa fizică de rețea, este un număr întreg pe 6 octeți (48 biți) pentru rețelele Token-ring sau Ethernet folosit la identificarea unui calculator într-o rețea locală. Inițial s-a dorit ca aceste adrese MAC să fie unice distribuindu-se zone contigue de adrese MAC la diferiți producători de interfețe de rețea. În prezent, adresele MAC sunt configurabile, aşa că dezideratul privind unicitatea lor a nu se mai poate realiza. Permit serverelor de DHCP să confirme dacă un calculator are permisiunea de a accesa rețeaua. Formatul adreselor MAC: XX–XX–XX–XX–XX–XX, unde X = {0-9;A-F}.

Maşină virtuală = implementare software a unei maşini (computer) ce are capacitatea de a executa programe ca un computer propriu-zis.

Network (Rețea): O combinație de calculatoare independente sau alte dispozitive, medii de comunicație cu fir sau fără fir şi echipamente conectate care permit schimbul şi partajarea de date sau resurse.

Password-Protected File: Un fişier configurat pentru a interzice accesul utilizatorilor care nu introduc parola validă de acces la conținutul fişierului.

PCMCIA: (Personal Computer Memory Card International Association). O organizație a producătorilor responsabilă cu promulgarea standardelor pentru diferite tipuri de circuite integrate incluzând cadrdurile PC şi cardurile Express.

Phishing: O metodă de fraudă întâlnită pe Internet care se desfăşoară prin intermediul e-mailurilor care conțin adrese şi legături către pagini web cu un conținut asemănător cu cel al unor instituții financiare bine cunoscute, cu scopul de a colecta informații despre conturile clienților, coduri de acces, parole, detalii despre cardurile de credit sau parole. Acestea sunt colectate şi utilizate apoi de infractori pentru deturnarea de fonduri din conturile reale ale clienților.

Phreaking: Metodă de hacking a sistemelor de telefonie clasice.

Port: O interfață logică sau fizică prin intermediul căruia un calculator comunică cu alte calculatoare din rețea, servere şi servicii sau cu dispozitivele periferice sau ataşate. Porturile de comunicație se împart în porturi de comunicație TCP sau UDP şi sunt de la 1 la 65535. Porturile cele mai cunoscute şi utilizate sunt cele de la 1 la 1024. Exemple de porturi de comunicație TCP: 22 SSH, 25 SMTP, 80 HTTP, 443 HTTPS dar şi porturi înalte precum 1433 SQL Server, 1521 Oracle, 3389 RDP.

Probă digitală: Informații şi date stocate sau transmise în format binar care pot fi introduse şi invocate într-o instanță de judecată.

Probă electronică: Date sau informații cu valoare pentru o investigație care este stocată sau transmisă pe sau de pe un dispozitiv electronic.

Protocol: Un set de reguli care guverneaza fluxul de informatie intr-o infrastructura de comunicatii.

Quarantine: Starea unei entități informaționale sau mai precis unui fişier, până la luarea deciziei de utilizare a acestuia.

Remote: Fişiere, dispozitive şi alte resurse care nu sunt conectate direct la un calculator dar care sunt utilizate ca şi când ar fi locale.

Screen Name: Un nume ales de un utilizator al Internetului folosit în comunicare. El poate fi numele real al unei persoane, o variațiune de la numele real sau poate fi un pseudonim (handle). Screen name-urile sunt utilizate pentru mesageria instant (IM) sau pentru autentificarea pe diferite site-uri web.

Server = program de aplicație care furnizează servicii altor aplicații (numite aplicații client), aflate pe acelaşi calculator sau pe calculatoare diferite.

Server: Un calculator cu o arhitectura specifica sau o statie de lucru sau host care executa servicii pentru clientii din retea

Sistem de operare: O aplicație specializată care permite controlul dispozitivelor fizice ale calculatorului şi facilitează instalarea şi rularea aplicațiilor de alte tipuri. Cele mai cunoscute nume de sisteme de operare: familia Microsoft® Windows (XP, Vista®, 7, Server 2008), familia produselor open-source: Linux, Suse, Unix, Solaris şi sistemele de operare and Apple® MacOS. În ultimii ani datorită exploziei dispozitivelor mobile intelogente şi cu performanțe hardware ridicate se utilizează din ce în ce mai mult sistemul de operare Android cu diferite variante ale sale. Pentru telefoane mobile un sistem de operare foarte răspândit este Symbian.

Smart Card: Cunoscut şi sub numele de card cu chip sau card cu un circuit integrat, care permite accesul la calculatoare sau locații securizate.

Software: Aplicații pentru calculatoare destinate efectuării anumitor operațiuni sau funcții specifice, precum: procesare de text, contabilitate, gestiunea rețelei, dezvoltarea site-urilor web sau a alor aplicații, gestiunea fişierelor, redarea conținutului multimedia şi altele.

Steganography: O metodă de a ascunde anumite fişiere sau informații în structura altor fişiere de alt tip sau altă natură.

Switch: Echipament de retea care conecteaza doua sau mai multe segmante de retea permitind traficul numai atunci cind este necesar. Switch-urile citesc eticheta (antetul) pachetelor si decid daca sa le transmita sau sa le blocheze in functie de destinatia pachetului.

USB: (Universal Serial Bus). O interfață de comunicare standard a calculatoarelor care permite interconectarea unui număr variat de dispozitive fizice sau medii de stocare şi comunicare precum: tastatura, mouse, scanner, imprimante, hard-discuri externe, telefoane mobile sau chei fizice de protecție.

Virtualizare = Virtualizarea este un concept ce presupune rularea unui sistem de operare pe maşini (computere) virtuale simulate cu ajutorul unor aplicații software dedicate. Aceste aplicații pot emula funcționarea tuturor componentelor unui sistem informatic real (FDD, CD-ROM, HDD, memorie, CPU, dispozitive USB, placa de rețea).

Virus: O aplicație capabilă să se ascundă, multiplice şi răspândească automat prin intermediul mediilor de interconectare sau transfer de date a calculatoarelor. Scopul lor este de a produce stricăciuni, de a fura informații sau de a prelua controlul altor calculatoare.

VoIP: (Voice over Internet Protocol). Tehnologie utilizată pentru a transmite conversații de tip voce prin intermediul liniilor de transmisie de rețea clasice.

Wireless: Orice dispozitiv fizic care poate accesa o rețea de date fără a folosi un mediu de comunicare conectat fizic.

Zip® File: Un tip de fişier compresat, care are o dimensiune mai mică decât fişierul original încorporat în arhiva Zip. Este utilizat pentru a transmite mai rapid informațiile prin intermediul mediilor de comunicare sau pentru a reduce spațiul de stocare de pe un mediu de stocare. Anumite arhive zip pot să aibă extensia EXE, ceea ce înseamnă că sunt arhive autoexecutabile şi nu au nevoie de un program de decompresare pentru a putea să pună la dispoziție conținutul original al fişierului compresat.

Indexul figurilor

Figura nr. 2.1 – *Volatilitatea probelor digitale* 14
Figura nr. 3.1 – *Diferite tipuri de dispozitive de calcul* 17
Figura nr. 3.2 - *Componentele interne ale unui hard disk (Sursa: http://www.hdd-tool.com/hdd-basic/hard-disk-and-hard-drive-physical-components.htm)* 18
Figura nr. 3.3 – *Structura hard discului* 19
Figura nr. 3.4 – *Tipuri de hardiscuri* 20
Figura nr. 3.5 – *Fişe de date pentru interconectarea hardiscurilor* 20
Figura nr. 3.6 – *Banda magnetică* 21
Figura nr. 3.7 – *Diferite tipuri de unităţi de stocare a datelor* 22
Figura nr. 4.1 - *Modelul de comunicare între filosofi* 25
Figura nr. 5.1 – *Procedura de colectare a probelor informatice* 39
Figura nr. 7.1 – *Identificarea sistemului de fişiere folosit pe o unitate de stocare* 45
Figura nr. 7.2 – *Lista de control acces asupra fişierului de pe discul E* 46
Figura nr. 7.3 – *Permisiunile efective pe un fişier* 47
Figura nr. 7.4 – *Fereastra de criptare a discurilor* 48
Figura nr. 7.5 – *Fereastra disk Quota* 49
Figura nr. 7.6 - *Compresia şi/sau criptarea fişierelor* 50
Figura nr. 7.7 - *Comanda compact* 50
Figura nr. 7.8 - *Feresatra pentru montarea discurilor* 51
Figura nr. 7.9 – *Specificarea acţiunilor de indexare a fişierelor pe de un disc* 52
Figura nr. 7.10 – *Serviciile de indexare în Windows XP* 52
Figura nr. 7.11 – *Serviciul de indexare în Windows 7* 53
Figura nr. 7.12 – *Informaţii despre sistem în formatul linie de comandă* 54
Figura nr. 7.13 – *Fereastra Registry Editor* 55
Figura nr. 7.14 – *Determinarea corectă a tipului unui fişier* 58
Figura nr. 7.15 – *Blocarea la scrierea pe dispozitive de stocare* 59
Figura nr. 8.1- *Opţiunile unui mesaj electronic în Microsoft Office Outlook* 62
Figura nr. 8.2 – *Afişarea opţiunilor unui mesaj de e-mail în Gmail* 62
Figura nr. 8.3 – *Detaliile unui mesaj de e-mail* 63
Figura nr. 8.4 – *Urmărirea mesajelor de pe un server de email Exchange* 65
Figura nr. 8.5 – *Lista detaliată de mesaje între doi utilizatori (Exchange Server)* 65
Figura nr. 8.6 – *Afişarea detaliilor despre un anumit mesaj* 66
Figura nr. 8.7 – *Schimbul complet de mesaje între doi utilizatori pe un anumit subiect* 66
Figura nr. 9.1 – *Istoricul dispozitivelor amovibile care au fost introduse într-un sistem de calcul* 67
Figura nr. 9.2 – *Detalii despre un anumit dispozitiv amovibil* 68
Figura nr. 9.3 – *Alte detalii despe istoricul dispozitivelor amovibile* 68
Figura nr. 9.4 – *Utilitarul USBDeview* 68
Figura nr. 9.5 – *Fişierul jurnal setupapi.log* 69
Figura nr. 9.6 – *Cheia de registry FriendlyName* 69
Figura nr. 9.7 – *Detalii despre dispozitivele amovibile în USBDeview* 69
Figura nr. 9.8 – *Proprietăţile unui fişier înainte de copierea pe un dispozitiv extern* 70
Figura nr. 9.9 – *Proprietăţile unui fişier după copierea pe dispozitive externe* 71
Figura nr. 10.1 – *Procesarea evidenţelor electronice în FTK* 80
Figura nr. 12.1 – *Arhivarea cu 7ZIP* 89
Figura nr. 12.2 - *Eroare la rularea executabilului joc.exe* 90
Figura nr. 12.3 - *Semnăturile digitale ale fişierelor de tip ZIP şi EXE* 91
Figura nr. 12.4 - *Semnătura digitală a unui fişier ZIP a cărui număr magic a fost modificat* 91
Figura nr. 12.5 - *SO Windows „vede" fişierul ca pe o aplicaţie* 92

Figura nr. 12.6 - *Modificarea registrilor calculatorului pentru a bloca scrierea stickurilor de memorie* 94
Figura nr. 12.7 - *Calculul valorii MD5 inițiale cu FTK Imager* 95
Figura nr. 12.8 - *Valoare MD5 stick memorie* 95
Figura nr. 12.9 - *Valoarea MD5 după clonare* 96
Figura nr. 12.10 - *Montarea imaginii cu FTK Imager* 97
Figura nr. 13.1 - *Fereastra de proprietăți a unei categoriei de mesaje Application.* 102

Bibliografie selectivă

Brian Carrier. *File System Forensic Analysis*. Addison-Wesley, 2nd edition, June 2005.

Dobrinoiu, M., *Infracțiuni în domeniul informatic*, Ed. CH Beck, Bucureşti, 2006

Eoghan C., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Second Edi tion, Academic Press, 2004

Fundamental Computer Investigation Guide for Windows, microsoft.com/technet/SolutionAccelerators, 2007, (paperback)

Hal Berghel, David Hoelzer, and Michael Sthultz. *Data Hiding Tactics for Windows and Unix File Systems*. http://berghel.net/publications/datahiding/datahiding.php.

HPA and DCO. International Journal of Digital Evidence, 5(1), 2006.

John Vacca. Computer Forensics: Computer Crime Scene Investigation. Charles River

Keith Jones. *Forensic Analysis of Internet Explorer Activity Files*, http://www.foundstone.com/pdf/wp index dat.pdf.

Ken C. Pohlmann, *The compact disc: a handbook of theory and use*, A-R Editions, Inc., 1989

Matthew Meyers and Marc Rogers. *Computer Forensics: The need for Standardization and Certification. International Journal of Digital Evidence*, 3(2), 2004.

Mayank R. Gupta, Michael D. Hoeschele, and Marcus K. Rogers. *Hidden Disk Areas: Media Inc*, 2nd edition, 2005.

Origins and Successors of the Compact Disc Contributions of Philips to Optical Storage, Series: Philips Research Book Series, Vol. 11

Peek, J.B.H., Bergmans, J.W.M., Haaren, J.A.M.M. van, Toolenaar, F., Stan, S.G., Springer 2009,

Toader, T., *Codul Penal. Codul de Procedură Penală*, Ed. Hamangiu, Bucureşti, 2010

Toader, T., *Drept penal român. Partea specială, Editia a -3-a*, Editura Hamangiu, Bucureşti, 2008

Vasiu, I., Vasiu, L., *Informatică Judiciară şi Drept informatic*, Ed. Albastră, Cluj-Napoca, 2007